L’impatto del Regolamento Europeo della Protezione dei Dati Personali sull’Organizzazione degli Enti Locali

Il Regolamento Generale sulla Protezione

dei dati personali (Regolamento UE 679/2016 - di seguito indicato “RGPD”) è un atto con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini, sia all’interno che all’esterno dei confini dell’Unione europea (ART.3 regolamento).

L’impatto del Regolamento Europeo della Protezione dei Dati Personali sull’Organizzazione degli Enti Locali

Perché si è sentito il bisogno di introdurre una nuova normativa in materia di tutela dei dati personali?

La risposta la si trova nel fatto che la continua introduzione di nuove tecnologie ha profondamente cambiato la società in cui viviamo: se prima quindi il tema della protezione del dato aveva ricadute in campo prettamente giuridico, adesso le possibili conseguenze interessano anche l’ambito politico, economico e sociale. **È sufficiente riflettere sul fatto che ai tempi dell’introduzione del D.Lgs. 196/2003, il cosiddetto Codice della privacy, la maggior parte delle informazioni venivano ancora scambiate via fax e l’utilizzo della posta elettronica era ancora molto limitato.**

Ai giorni nostri invece la maggior parte delle attività che svolgiamo, che siano a scopo lavorativo o esclusivamente personale, passano attraverso strumenti informatizzati e attraverso internet, e ognuna di queste attività prevede il trasferimento e il trattamento di enormi quantità di dati personali a noi riconducibili

Il testo, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, diventerà definitivamente applicabile in via diretta in tutti i Paesi UE **a partire dal 25 maggio 2018**.

Il RGPD è parte del cosiddetto "Pacchetto protezione dati personali", l'insieme normativo che definisce un nuovo quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'UE e comprende anche **la Direttiva in materia di trattamento dati personali nei settori di prevenzione, contrasto e repressione dei crimini.**

Dal 25 maggio 2018, anche per gli enti locali, il RGPD andrà a sostituire la direttiva sulla protezione dei dati (ufficialmente Direttiva 95/46/EC) istituita nel 1995. Nell'ambito del nuovo quadro normativo che la Commissione europea ha voluto delineare e al quale gli Stati membri devono conformarsi, l'Italia ha recepito i nuovi principi attraverso l'art. 13 della legge delega n. 163/2017, entrata in vigore il 21 novembre 2017

Finalità dell’art. 13 della legge delega n. 163/2017, entrata in vigore il 21 novembre 2017

1) abrogare le disposizioni del Decreto Legislativo n. 196/2003 (l’attuale Codice Privacy) che siano in contrasto o comunque incompatibili con la nuova disciplina europea in tema di trattamento di dati personali e a modificarlo al fine di dare puntuale attuazione alle disposizioni del RGPD;

2)valutare l’opportunità di avvalersi dei poteri specifici del Garante per la protezione dei dati personali (di seguito Garante Privacy) affinché adotti provvedimenti attuativi e integrativi volti al perseguimento delle finalità previste dal RGPD;

3)adeguare l’attuale regime sanzionatorio, a livello penale e amministrativo, alle disposizioni del RGPD, al fine di garantire la corretta osservanza della nuova normativa.

Il Consiglio dei Ministri del 21 marzo ha approvato lo schema di un decreto legislativo di adeguamento della normativa nazionale alle disposizioni del Regolamento Europeo 2016/679, in esame preliminare e in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163),

Il decreto legislativo suddetto non ha ancora definito il suo iter, per cui *il Regolamento europeo 679/2016, direttamente applicabile in tutti gli Stati, anche in assenza di emanazione di decreti attuativi della delega, entrerà in vigore* **dal 25 maggio 2018.**

Il regolamento rimarrà in vigore fino a quando non sarà sostituito dal decreto legislativo di adeguamento.

Ambito di applicazione del Nuovo Regolamento – 1 ambito materiale

L’ambito materiale fa riferimento a quale tipologia di trattamenti si debba applicare il Regolamento.

Si applica ai trattamenti interamente o parzialmente automatizzati di dati personali, e quindi a tutti quelli effettuati tramite strumenti informatici ed elettronici, e ai trattamenti di dati personali non automatizzati.

Ma la norma fornisce un’ulteriore indicazione: si deve applicare al trattamento di dati che sono contenuti in un archivio o che sono destinati a figurarvi.

Ambito di applicazione del Nuovo Regolamento – 1 ambito territoriale

Se il soggetto che tratta i dati è stabilito nell'Unione si applica il Regolamento anche se il trattamento è effettuato al di fuori del territorio dell'Unione, cioè anche se delocalizza il trattamento dei dati.

Ambito di applicazione del Nuovo Regolamento – 2 ambito territoriale

La seconda circostanza prevede che, se il soggetto di cui si trattano i dati si trova nell'Unione, si debba applicare il Regolamento; questo però in due casi:

1)se il trattamento dei dati è finalizzato alla vendita di beni o servizi (anche a titolo gratuito);

2)se il trattamento riguarda il monitoraggio del comportamento dell'interessato all'interno dell'Unione.

Riguardo a quest'ultimo caso è necessario verificare che tipologia di monitoraggio viene effettuata, se vengono tracciate eventuali operazioni su internet o se addirittura siano messi in pratica trattamenti finalizzati alla profilazione dell'utente.

Definizione di dato personale - 1

Sono dati personali quindi tutte quelle informazioni che possono portare all'identificazione della persona in maniera diretta o, se incrociate tra loro, in maniera indiretta. Si parla di dati personali quindi quando si fa riferimento al nominativo di un individuo, al suo numero di identificazione (per esempio documento di identità), ai dati relativi all'ubicazione, che possono essere sì l'indirizzo di residenza, ma anche dati di geolocalizzazione, a eventuali identificativi online, come nickname e account, e a tutti quegli elementi caratteristici della identità fisica, fisiologica e psichica della persona che sono ricavabili da strumenti di rilevazione biometrica o da campioni biologici.

Definizione di dato personale – 2

Il Regolamento stabilisce che il trattamento di tutte le tipologie di dati personali debba essere effettuato con adeguate misure di sicurezza, garantendo in ogni momento la tutela della persona fisica a cui questi dati appartengono.

Il Regolamento definisce come ***"particolari categorie di dati"*** quei dati personali collegati a informazioni che riguardano gli aspetti più intimi della vita di un soggetto e che possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché quei dati genetici e biometrici che evidenziano in modo univoco una persona fisica e i dati relativi alla salute o all'orientamento sessuale della persona.

Il trattamento dei dati personali

È definito trattamento qualsiasi tipo di operazione o insieme di operazioni applicate a dati personali o insieme di dati personali. I trattamenti possono essere suddivisi in quattro fasi. **Una fase preliminare di raccolta e registrazione, una fase di elaborazione,** che comprende una serie di possibili operazioni con oggetto il dato (l'organizzazione, l'elaborazione, la modifica, l'estrazione, l'utilizzo), **una fase di circolazione, con la comunicazione e diffusione,** e una fase residuale inerente alla **conservazione o alla cancellazione e distruzione.** Ulteriore metodo per catalogare i trattamenti, non definito dalla normativa, è quello di organizzarli per finalità. A ogni trattamento corrisponde una finalità e per ogni finalità sono necessari dei trattamenti

Il trattamento dei dati personali – Principi 1

I dati personali devono essere trattati nel rispetto dei seguenti principi:

A) Trattati in modo lecito, corretto e trasparente.

Lecito nel senso che il trattamento deve sempre rispettare la normativa, sia quella generale che quella specifica; corretto, ossia che il trattamento deve essere effettuato rispettando norme etiche e deontologiche “non codificate”, assicurando sempre il rispetto delle esigenze dei soggetti interessati; trasparente, in modo che sia costantemente tutelata la consapevolezza dell’interessato.

B)Raccolti per finalità determinate ed esplicite.

Le finalità del trattamento devono essere predeterminate e chiare ed eventuali ulteriori trattamenti non devono avere finalità incompatibili con quella originaria.

C)Adeguati, pertinenti e limitati.

È il principio della minimizzazione dei dati; compatibilmente alla finalità ricercata i dati devono essere ridotti al minimo, deve essere effettuato il minor numero di trattamenti, deve essere ridotto al minimo il numero di soggetti che operano i trattamenti e la conservazione deve essere il più possibile limitata nel tempo.

Il trattamento dei dati personali – Principi 2

D) Esatti e aggiornati.

Condizione essenziale per poter effettuare un trattamento è che i dati siano sempre esatti e aggiornati; questo prevede altresì che si proceda sempre alla cancellazione di quelli non più utili e all'aggiornamento costante di quelli utilizzati per il trattamento.

E) Conservati per un periodo di tempo limitato.

Ci si collega al principio della minimizzazione citato precedentemente. I dati devono essere conservati per un periodo di tempo non eccedente quello necessario per raggiungere la finalità del trattamento. Ovviamente fanno eccezione i dati archiviati nel pubblico interesse, quelli per la ricerca scientifica e storica e per fini statistici.

F)Trattati con adeguate misure di sicurezza.

Deve sempre essere garantita l'integrità e la riservatezza nel tempo del dato mettendo in campo tutte quelle misure di sicurezza, tecniche e organizzative, adeguate. Il dato deve sempre essere protetto, perché attraverso la protezione del dato passa la protezione della persona fisica a cui il dato si riferisce.

Il trattamento dei dati personali – Principi 3

Il Regolamento introduce un importante principio, quello dell' *accountability, o responsabilizzazione, concetto che, in un solo* termine, attribuisce al titolare da una parte l'obbligo di rispettare quanto previsto dal Regolamento e dell'altra l'onere processuale della prova di averlo fatto.

La liceità del trattamento - 1

Le sei basi giuridiche sulle quali si deve basare un trattamento di dati in modo che questo si possa definire lecito, **possono essere suddivise in due categorie;**

1) la prima richiede che ci sia un **accordo contrattuale** o un incontro di volontà tra le parti interessate; è necessario che l'interessato esprima la sua opinione preventivamente sul singolo trattamento;

2)la seconda fonda le sue basi sulla presenza di una **norma di legge;** l'interessato può esclusivamente tutelarsi in un secondo momento nell'eventualità in cui il trattamento non sia conforme a quanto richiesto dalla normativa.

La liceità del trattamento - 2

Le basi giuridiche che rendono lecito il trattamento sono:

1)Consenso;

2)Contratto;

3)Obbligo di legge;

4) Salvaguardia interessi vitali;

5)Interesse legittimo;

6) Interesse pubblico.

La liceità del trattamento – consenso

Consenso dell'interessato

Il consenso dell'interessato (sempre revocabile) deve essere richiesto per una o più specifiche finalità. Deve essere espresso mediante un atto positivo inequivocabile con il quale l'interessato possa manifestare la sua intenzione libera e informata di accettare il trattamento di dati che lo riguardano. Può configurarsi attraverso una specifica dichiarazione scritta, anche attraverso mezzi elettronici, o orale. **Esempio: l' azienda/organizzazione offre un'app musicale e chiede il consenso dei cittadini a trattare le loro preferenze musicali per suggerire canzoni su misura ed eventuali concerti.** L'interessato ha inoltre sempre il diritto di revocare il proprio consenso in qualsiasi momento con gli stessi strumenti attraverso i quali il consenso è stato prestato. Per i minori di 16 anni il consenso deve essere prestato dai genitori o da chi ne fa le veci.

La liceità del trattamento – contratto – obbligo di legge

Contratto

L’esistenza di una fase pre-contrattuale o di un contratto assorbe al suo interno la necessità che venga prestato il consenso al trattamento dei dati. Ne consegue che in questo caso il trattamento dei dati dell’interessato sia necessario per gli adempimenti conseguenti alla sottoscrizione del contratto tra le parti. **Esempio: l’ azienda/organizzazione vende merci online. Può trattare i dati necessari per procedere, su richiesta dell’interessato prima della stipula del contratto e per l’esecuzione dello stesso. Potrà trattare il nome, l’indirizzo di consegna, il numero della carta di credito (se si esegue il pagamento con carta) etc..**

La liceità del trattamento – obbligo di legge

Obbligo di legge

La presenza di un obbligo di legge rende lecito il trattamento di dati effettuato per ottemperare agli obblighi da questa previsti.

Sono un esempio nel settore privato tutte le banche dati alimentate per gli obblighi previsti dalla normativa antiriciclaggio o gli invii di informazioni all'anagrafe tributaria dettati dalla normativa fiscale.

La liceità del trattamento – salvaguardia interessi vitali

Salvaguardia degli interessi vitali

Qualsiasi trattamento effettuato con il fine della salvaguardia di interessi vitali è lecito. La salvaguardia infatti di un bene supremo, come appunto è la vita, sospende la possibilità di non acconsentire al trattamento di dati personali.

Es: **un ospedale che cura un paziente dopo un grave incidente stradale non ha bisogno del suo consenso per cercare un documento e verificare se questa persona esiste nel database dell'ospedale e trovarne l’anamnesi, o per contattare il parente più prossimo**.

La liceità del trattamento – Legittimo interesse del titolare

Legittimo interesse del titolare

Un trattamento può essere effettuato da un titolare se il titolare ha un legittimo interesse nel farlo e non prevalgono interessi, diritti e libertà dell'interessato. Per la stessa casistica il Codice della Privacy prevedeva che fosse il Garante a stabilire l'elenco dei trattamenti effettuabili per legittimo interesse con apposito provvedimento, mentre con il Regolamento invece il legittimo interesse vive a prescindere dal parere dell'Autorità di Controllo ed è demandata alle figure interne di ogni organizzazione tenuta al rispetto della normativa **(principio di responsabilizzazione).**

Per esemplificare: se una società finanziaria cerca un suo cliente che è in ritardo coi pagamenti, ha il legittimo interesse ad ottenere il nuovo indirizzo del cliente, anche in assenza di consenso specifico. Il titolare del dato e lo detiene legittimamente, deve **bilanciare i suoi interessi con quelli dell'interessato**, e quindi il trattamento appare ingiustificato se ha degli effetti pregiudizievoli sui diritti e le libertà, o interessi legittimi, del singolo (**riportandoci all'esempio di prima, è evidente che l'interesse del cliente a non pagare le tasse non può essere ritenuto legittimo o giustificato**). La società finanziaria deve garantire che i dati siano precisi, aggiornati, non eccessivi e la società ottiene solo i dati necessari allo scopo, rintracciare il cliente)

La liceità del trattamento – interesse pubblico

Compiti di interesse pubblico per l'esercizio di pubblici poteri.

Rientrano in questa casistica tutti i trattamenti effettuati dalle Pubbliche Amministrazioni. **La Pubblica Amministrazione deve sempre essere in grado di evidenziare quali siano le norme sulla base delle quali vengono effettuati i trattamenti**. In nessun modo può contare di legittimare i suoi trattamenti con il consenso dell'interessato; ne consegue quindi che **o un trattamento effettuato dalla Pubblica Amministrazione è frutto di una disposizione normativa oppure quel trattamento è illegittimo.**

Trattamento di particolari categorie di dati (ex sensibili) - 1

Il Regolamento prevede che sia prestata una maggiore attenzione e siano dedicate specifiche misure di protezione a quei **dati che sono particolarmente sensibili**.

Tra questi dati particolari troviamo i dati personali atti a rivelare **l'origine razziale o etnica, le convinzioni religiose** o filosofiche, le opinioni politiche, l'appartenenza sindacale, ma anche i dati genetici e biometrici e quelli relativi alla salute o alla vita e orientamento sessuale.

Relativamente alla tipologia di dati sopra elencati il Regolamento **in linea di massima prevede il divieto di trattamento, salvo nel caso in cui ricorrano specifiche condizioni di seguito elencate.**

Trattamento di particolari categorie di dati (ex sensibili) - Consenso

Consenso

Il trattamento di particolari categorie di dati (ex sensibili) è legittimo nel caso in cui il soggetto interessato abbia prestato esplicito consenso relativamente a una o più finalità specifiche. **Il consenso prestato attraverso un comportamento concludente non può mai essere considerato esplicito, a differenza del trattamento dei dati personali non considerati particolari.**

Trattamento di particolari categorie di dati (ex sensibili) - **Obblighi in materia di diritto di lavoro, sicurezza sociale, protezione sociale**

Obblighi in materia di diritto di lavoro, sicurezza sociale, protezione sociale.

Il trattamento di particolari categorie di dati è legittimo nel caso in cui sia necessario per assolvere obblighi ed esercitare diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia **autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo,** in presenza di adeguate garanzie per i diritti fondamentali e gli interessi dell'interessato. **(Es: un'azienda con dipendenti, per ottenere la copertura previdenziale, la legge ti obbliga a fornire dati personali (ad esempio, il reddito settimanale dei dipendenti) all'autorità competente.**

Trattamento di particolari categorie di dati (ex sensibili) – Tutela di interessi vitali

Tutela di interessi vitali

Il trattamento di particolari categorie di dati è legittimo se necessario a tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso.

Trattamento di particolari categorie di dati (ex sensibili) – Organizzazione e associazioni no profit

Organizzazione e associazioni no profit

Il trattamento di particolari categorie di dati è legittimo se 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, religiose o sindacali, **a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e *che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato.***

Trattamento di particolari categorie di dati (ex sensibili) – Dati pubblici e Diritto di difesa

Dati pubblici

Il trattamento di particolari categorie di dati è legittimo se riguarda dati personali resi manifestamente pubblici dall'interessato (Es: il malato di Sla che si presenta ad una manifestazione televisiva, etc.)

Diritto di difesa

Il trattamento di particolari categorie di dati è legittimo se è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali.

Trattamento di particolari categorie di dati (ex sensibili) – interesse pubblico

Interesse pubblico

Il trattamento di particolari categorie di dati è legittimo se è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che **deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Es: dati trattati nell'ambito di procedimento disciplinare da parte di un ordine professionale.**

Trattamento di particolari categorie di dati (ex sensibili) – Sanità

Sanità

Il trattamento di particolari categorie di dati è legittimo quando è necessario per finalità di medicina preventiva o di medicina del lavoro**, valutazione della capacità lavorativa del dipendente**, **diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.

Trattamento di particolari categorie di dati (ex sensibili) – Statistica, ricerca storica e scientifica

Statistica, ricerca storica e scientifica

Il trattamento di particolari categorie di dati è legittimo se effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici a patto che **sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (Es: dati relativi ai tumori in un determinato ambito territoriale).**

Trattamento di particolari categorie di dati (ex sensibili) – Trattamento di dati giudiziari

Trattamento di dati giudiziari

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza **deve avvenire soltanto sotto il controllo dell'autorità pubblica o nel caso in cui il trattamento sia autorizzato dal diritto dell'Unione o degli Stati membri prevedendo garanzie appropriate per i diritti e le libertà degli interessati.** Un eventuale registro completo delle condanne penali (per esempio il casellario giudiziale) deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Diritti degli interessati e principi

Il Regolamento riconosce al soggetto interessato i diritti di seguito riportati:

1)trasparenza;

2)informativa;

3)accesso;

4)rettifica;

5)cancellazione/oblio;

6)limitazione del trattamento;

7)portabilità dei dati;

8)opposizione al trattamento.

Trasparenza e informazione 1-2

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

L'interessato deve essere messo in condizione di poter ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta del dato o comunque entro un tempo ragionevole nel caso in cui i dati non siano da lui direttamente forniti.

Assenza di obbligo di informazione

Per contro, non è necessario imporre l'obbligo di fornire l'informativa se l'interessato dispone già dell'informazione, **se la registrazione o la comunicazione dei dati personali sono previste per legge o se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato.**

Quest'ultima eventualità potrebbe verificarsi, ad esempio, nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi si può tener conto del numero di interessati, dell'antichità dei dati e di eventuali garanzie adeguate in essere.

Diritto accesso - 3

L’interessato ha il diritto di accedere ai propri dati personali e avere informazioni a riguardo delle finalità e delle modalità di trattamento, al fine di poterne facilmente verificare la liceità.

Nel caso in cui il titolare del trattamento tratti una notevole quantità di dati che riguardano il soggetto interessato, può far richiesta all’interessato di specificare le informazioni o le attività di trattamento alle quali la richiesta si riferisce.

Le informazioni relative ai dati per le quali l’interessato può presentare richiesta sono: 1) le finalità del trattamento; 2) le categorie di dati personali in questione; 3) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi od organizzazioni internazionali; 4) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; 5) l’esistenza del diritto dell’interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; 6) il diritto di proporre reclamo a un’Autorità di controllo; 7) qualora i dati non siano raccolti presso l’interessato, tutte le informazioni disponibili sulla loro origine; 8) l’esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l’importanza e le conseguenze previste di tale trattamento per l’interessato.

Diritto di rettifica - 4

Un ulteriore diritto esercitabile dall'interessato è **il diritto alla rettifica, senza ingiustificato ritardo, dei dati personali inesatti trattati dal titolare del trattamento.** Con rettifica si intende non solo la correzione di dati inesatti o il loro aggiornamento, ma anche l'integrazione di dati personali incompleti in seguito a presentazione da parte dell'interessato di apposita dichiarazione integrativa.

A meno che l'attività non comporti uno sforzo spropositato o un costo insostenibile, il titolare del trattamento deve comunicare tale aggiornamento anche a tutti i destinatari a cui ha trasmesso i dati.

Diritto alla cancellazione dei dati – 5

L’interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano se la conservazione di tali dati è effettuata in violazione del Regolamento.

Nello specifico l’interessato ha il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali nel caso si verifichi una di queste situazioni: 1) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; 2) l’interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; 3) l’interessato si oppone al trattamento nei casi previsti dal Regolamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; 4) i dati personali sono stati trattati illecitamente; 5) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento; 6) i dati personali sono stati raccolti relativamente all’offerta di servizi della società dell’informazione di cui all’articolo 8, paragrafo 1, del Regolamento.

Tale diritto è particolarmente rilevante se l’interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. Il diritto alla cancellazione dei dati non è esercitabile nel caso in cui l’ulteriore conservazione dei dati personali sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell’esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

Diritto all'oblio – 5 bis

Il Regolamento prevede inoltre che **il diritto di cancellazione sia estendibile anche nell'ambiente online, configurandosi come "diritto all'oblio"**: il titolare del trattamento che ha pubblicato dati personali è quindi tenuto a informare i titolari del trattamento che trattano tali dati personali e dare indicazione di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali.

Nel fare questo è opportuno che **il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.**

Limitazione del trattamento - 6

Il diritto alla limitazione del trattamento (ad esempio andando a limitare il trattamento del dato alla sola conservazione, escludendo qualsiasi altro utilizzo), è un diritto che l'interessato può esercitare, a propria tutela, nel caso in cui: **1) l'interessato contesti l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;** 2) il trattamento sia illecito e l'interessato si opponga alla cancellazione dei dati personali e chieda invece che ne sia limitato l'utilizzo; 3) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; 4) l'interessato si sia opposto al trattamento in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato. **L'interessato che ha ottenuto la limitazione del trattamento deve essere avvisato con apposita comunicazione dal titolare del trattamento dell'avvenuta limitazione e, in seguito, nel caso in cui questa venga revocata**

Portabilità dei dati - 7

L’esercizio del diritto alla portabilità prevede anche che i dati forniti dall’interessato a un titolare del trattamento siano trasmissibili a un altro titolare del trattamento senza alcuna forma di impedimento.

Tale diritto è esercitabile qualora l’interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l’esecuzione di un contratto. Non deve applicarsi nel caso in cui il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto.

Opposizione al trattamento - 8

Il Regolamento prevede che l'interessato possa esercitare il diritto di opposizione al trattamento dei propri dati personali e identifica tre differenti tipi di opposizione.

Nella *prima tipologia è considerato il diritto di opposizione, per motivi* connessi alla situazione particolare dell'interessato, relativo a quei trattamenti che lo riguardano effettuati per scopi di interesse pubblico o legittimo interesse del titolare, profilazione compresa. **Si fa riferimento quindi a trattamenti legittimati da basi giuridiche diverse dal consenso, per i quali è necessario che il titolare confronti i motivi che permettono il trattamento rispetto alle ragioni dell'interessato**. Nel caso in cui, da questo confronto, si stabilisca una prevalenza delle ragioni dell'interessato, il titolare dovrà astenersi dall'effettuare qualsiasi ulteriore trattamento di dati personali.

La *seconda tipologia di opposizione esercitabile è quella che si riferisce a* trattamenti effettuati per finalità di **marketing diretto.** Relativamente a questo tipo di trattamenti **il soggetto interessato ha sempre il diritto di opporsi al trattamento dei propri dati personali.**

La *terza e ultima tipologia prende in considerazione l'opposizione al trattamento* di dati personali con finalità di ricerca scientifica o storica o a fini statistici. In questo caso il soggetto interessato, per motivazioni connesse a una propria situazione particolare, ha **il diritto di opporsi al trattamento di dati personali che lo riguardano tranne nei casi in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.**

Novità del Nuovo Regolamento Europeo (RGPD)

Le disposizioni contenute nel nuovo Regolamento europeo per la protezione dei dati personali impongono alle Pubbliche Amministrazioni di assicurare, come già detto, entro il 25 maggio 2018, l'applicazione tassativa della normativa europea sul trattamento dei dati, **la cui responsabilità ultima cade sul titolare del trattamento, figura che negli enti locali è ricoperta dal Sindaco.**

Attuazione delle nuove disposizioni per le Amministrazioni locali - difficoltà operative.

L’adozione delle disposizioni contenute nel Regolamento europeo, infatti, inciderà notevolmente sulla loro organizzazione interna, modificandone gli assetti strutturali, la ricognizione e la valutazione delle misure sicurezza normative, organizzative e tecnologiche, già adottate dagli enti a tutela della privacy.

1 - Le principali novità introdotte dal Regolamento Generale sulla Protezione dei dati personali (RGPD)

1)è introdotta la responsabilità diretta dei titolari del trattamento in merito al compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali, **richiedendosi un approccio proattivo della tutela della sicurezza dei dati personali;**

2)è definita la nuova categoria di dati personali (i c.d. dati sensibili di cui al precedente Codice Privacy);

3)viene istituita la figura obbligatoria del Responsabile della protezione dei dati, incaricato di assicurare una gestione corretta dei dati personali negli enti.

Tale figura può essere individuata tra il personale dipendente in organico, oppure è possibile procedere a un affidamento all'esterno, in base a un contratto di servizi;

2 - Le principali novità introdotte dal Regolamento Generale sulla Protezione dei dati personali (RGPD)

- 4)viene introdotto il Registro delle attività del trattamento ove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate dall'ente. Il Registro dovrà contenere specifici dati indicati dal RGPD;

- 5)viene richiesto agli enti l'obbligo, prima di procedere al trattamento, di effettuare una valutazione di impatto sulla protezione dei dati. Tale adempimento è richiesto quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. (Si pensi, ad esempio, ai dati ottenuti dalla sorveglianza di zone accessibili al pubblico).

I soggetti ed i nuovi strumenti.

Il RGPD ridisegna, in particolare, il ruolo, i compiti e le responsabilità del Titolare e del Responsabile del trattamento dei dati personali in relazione ai nuovi principi e strumenti introdotti dallo stesso e **individua la nuova figura del Responsabile della protezione dei dati.**

Il Titolare del trattamento
(Il Sindaco)

Il Titolare del trattamento (cioè il Sindaco o suo delegato) dei dati personali raccolti o meno in banche dati, automatizzate o cartacee, è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del RGPD: ***liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.***

Privacy by design

Il Sindaco (o suo delegato), deve mettere in atto le ***misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia effettuato in modo conforme al RGPD.***

Le misure sono definite fin dalla fase di progettazione (DATA PROTECTION BY DESIGN) e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Privacy by default

La privacy by default, è invece relativo al fatto che il titolare del trattamento (o suo delegato) deve organizzare il sistema di tutela della protezione dei dati in modo tale da garantire l'adozione di misure tecniche o organizzative che, **per impostazione predefinita,** consentano il trattamento dei soli dati strettamente necessari per il raggiungimento di ogni specifica finalità. L'esemplificazione si può trovare nell'adozione di sistemi gestionali informatici che prevedano la possibilità di rispondere alle richieste di accesso ai dati, contemplando come procedure predefinite quella di estrazione e comunicazione dei dati all'interessato oppure **sistemi che prevedano tempistiche per la conservazione di dati adeguate alla tipologia di trattamento di dati effettuata.**

Il Responsabile del trattamento

Il Responsabile del trattamento (Uno o più Dirigenti/Quadri/Responsabili di U.O. delle strutture di massima dimensione) in cui si articola l'organizzazione del Comune, è nominato dal Sindaco Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza.

Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative di cui all'art. 5 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

Sub-responsabili del trattamento **(gli incaricati del trattamento nel Codice Privacy)**

E’ consentita la nomina di sub-responsabili del trattamento **(gli incaricati del trattamento nel Codice Privacy)** da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario;

le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l’ambito del trattamento consentito.

Responsabilità nel trattamento dei dati personali

Il Responsabile risponde, anche dinanzi al Titolare (Sindaco), dell'inadempimento dell'operato del sub responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, **salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sul suo operato.**

Il Responsabile della protezione dei dati

L’istituzione della nuova figura del Responsabile della protezione dei dati (“RPD” o DPO – Data Protection Officier) è la principale novità normativa del Regolamento europeo che **mira al potenziamento del controllo dell’efficacia e della sicurezza dei sistemi di protezione dei dati personali.**

Requisiti Responsabile Protezione Dati

- RPD può essere scelto fra i dipendenti del Comune di qualifica non inferiore alla cat. D (oppure C negli enti di minore dimensione), purché in possesso di idonee qualità professionali, con **particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati**, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale

Requisiti Responsabile Protezione Dati

- **In assenza all'interno dell'ente di figura idonea, l**'incarico può essere conferito a soggetto esterno (anche operatore economico diverso da persona fisica che però deve indicare il soggetto che assumerà l'incarico) mediante procedura rispettosa del codice dei contratti pubblici.
- Il soggetto che partecipa alla procedura deve garantire e dimostrare le qualità professionali necessarie ad assumere l'incarico. I piccoli comuni possono ricorrere a convenzione tra di loro e anche tramite unione già esistente.

Responsabile Protezione Dati

Il pacchetto da affidare all'esterno, può comprendere:

A) l' incarico di RPD (DPO) e la valutazione di impatto sulla protezione dei dati.

B) La mappatura dei processi, per individuare quelli collegati al trattamento dei dati personali; l' individuazione, tra i processi risultanti dalla mappatura, di quelli che presentano rischi, con una prima valutazione degli stessi i termini di maggiore o minore gravità; mappatura degli incarichi dei soggetti coinvolti nel trattamento e dei livelli di responsabilità, ed eventuale aggiornamento; l' elaborazione del piano di adeguamento complessivo, contenente le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi (se necessario) e dei tempi previsti, nonché delle attività di monitoraggio; la predisposizione del registro dei trattamenti di dati personali e del registro delle categorie di attività;

C) gli interventi formativi del personale; la proposta di adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni.

1 - Compiti del Responsabile Protezione Dati

Il Responsabile della protezione dei dati è incaricato, infatti, dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento;

2 - Compiti del Responsabile Protezione Dati

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità;

f) verificare la tenuta dei registri del Titolare e del/dei Responsabili sul trattamento.

1) I nuovi strumenti: il registro delle attività di trattamento

Il Registro delle attività di trattamento svolte dal Comune quale Titolare del trattamento (da tenere in forma scritta e formato elettronico), reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, eventualmente del Contitolare del trattamento, del RPD;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute);

2) I nuovi strumenti: il registro delle attività di trattamento

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica; autorità pubblica; altro organismo destinatario;

e) l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

1 - Il Registro delle categorie di attività

Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento reca le seguenti informazioni:

a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD;

b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione;

2- Il Registro delle categorie di attività

c) l’eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l’uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare, prima di effettuare il trattamento, deve effettuare una valutazione dell’impatto del medesimo trattamento ai sensi dell’art. 35, RGDP, considerati la natura, l’oggetto, il contesto e le finalità dello stesso trattamento.**

La Valutazione di impatto sulla protezione dei dati.

Una valutazione di impatto sulla protezione dei dati consiste in una procedura finalizzata a **descrivere il trattamento, valutarne necessità e proporzionalità, facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali e permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.**

Data breach (violazione dati personali)

Il Regolamento prevede che un'eventuale violazione dei dati personali (*data breach) debba essere affrontata dal* ***titolare del trattamento in*** **modo adeguato e tempestivo,** al fine di scongiurare danni fisici, materiali o immateriali alle persone fisiche. l titolare del trattamento, venuto a conoscenza di una violazione dei dati personali, **deve notificare tale violazione all'autorità di controllo, senza ingiustificato ritardo e, ove possibile, entro 72 ore, a meno che non sia in grado di dimostrare, conformemente al principio di responsabilizzazione, che la violazione non possa presentare un rischio per i diritti e le libertà dei soggetti interessati**. Oltre il termine di 72 ore, tale notifica deve essere corredata delle ragioni del ritardo, permanendo comunque l'obbligo di trasmettere le informazioni mancanti non appena disponibili.

Adempimenti che è necessario porre in essere per adeguare il sistema al nuovo regolamento in vigore dal 25 maggio 2018

I primi adempimenti che è necessario porre in essere sono:

1) la nomina del RPD;

2) l’adozione del Registro dei trattamenti di dati personali (obbligatorio per il Titolare) e del Registro delle categorie di attività trattate da ciascun Responsabile del trattamento, che hanno contenuti obbligatori previsti specificamente dal RGPD. I registri possono comprendere anche altre informazioni non obbligatorie, al fine di garantire il perfetto allineamento con i principali “oggetti” (mappa dei processi, organigramma dell’ente, portafoglio fornitori, mappa degli applicativi);

Adempimenti che è necessario porre in essere per adeguare il sistema al nuovo regolamento in vigore dal 25 maggio 2018

3) la mappatura dei processi. Tutte le informazioni raccolte per definire i contenuti dei Registri saranno utili anche successivamente, quando andranno identificati e valutati i principali gaps da colmare per essere conformi al RGPD;

4)definire e redazione, alla luce dei divari evidenziati, un piano di adeguamento complessivo (action plan), compresa la stesura ex novo della documentazione o modifica della documentazione esistente (ad esempio informative, moduli di consenso, clausole contrattuali) e avvio della relativa adozione, anche verso l'esterno;

5)attuazione e conseguente monitoraggio degli interventi previsti.

Adempimenti che è necessario porre in essere per adeguare il sistema al nuovo regolamento in vigore dal 25 maggio 2018

Il processo di adeguamento al regolamento può essere attuato seguendo lo schema indicato di seguito.

1)Struttura organizzativa:, formalizzazione e implementazione del sistema di data protection, sia a livello di **della struttura organizzativa**macro-struttura sia a livello di micro-struttura (ruoli e responsabilità);

2)soggetti coinvolti: sensibilizzazione e formazione dei soggetti chiamati a ricoprire un ruolo attivo nell'ambito del modello di funzionamento della data protection, ma anche dei soggetti del Comune indirettamente coinvolti nella protezione dei dati personali;

Adempimenti che è necessario porre in essere per adeguare il sistema al nuovo regolamento in vigore dal 25 maggio 2018

3) processi: definizione, formalizzazione e implementazione di processi e regole connessi alla protezione dei dati personali, sia in modo diretto (ad esempio la gestione dei diritti degli interessati) sia in modo indiretto (ad esempio la gestione delle misure di sicurezza tecnico-organizzative);

4) documentazione: stesura ex novo della documentazione o modifica della documentazione esistente (ad esempio informative, moduli di consenso, clausole contrattuali) e avvio della relativa adozione, anche verso l'esterno;

Adempimenti che è necessario porre in essere per adeguare il sistema al nuovo regolamento in vigore dal 25 maggio 2018

5)controlli interni: definizione e implementazione di un sistema di controlli interni per la protezione dei dati personali (ad esempio il sistema di deleghe), ivi compresa la realizzazione di internal audit volti a evidenziare eventuali non conformità. A valle dell'intero processo di adeguamento deve essere quindi effettuato un controllo periodico in merito alla corretta adozione del modello di funzionamento della data protection ed elaborazione di eventuali azioni correttive, con conseguente aggiornamento del modello stesso.