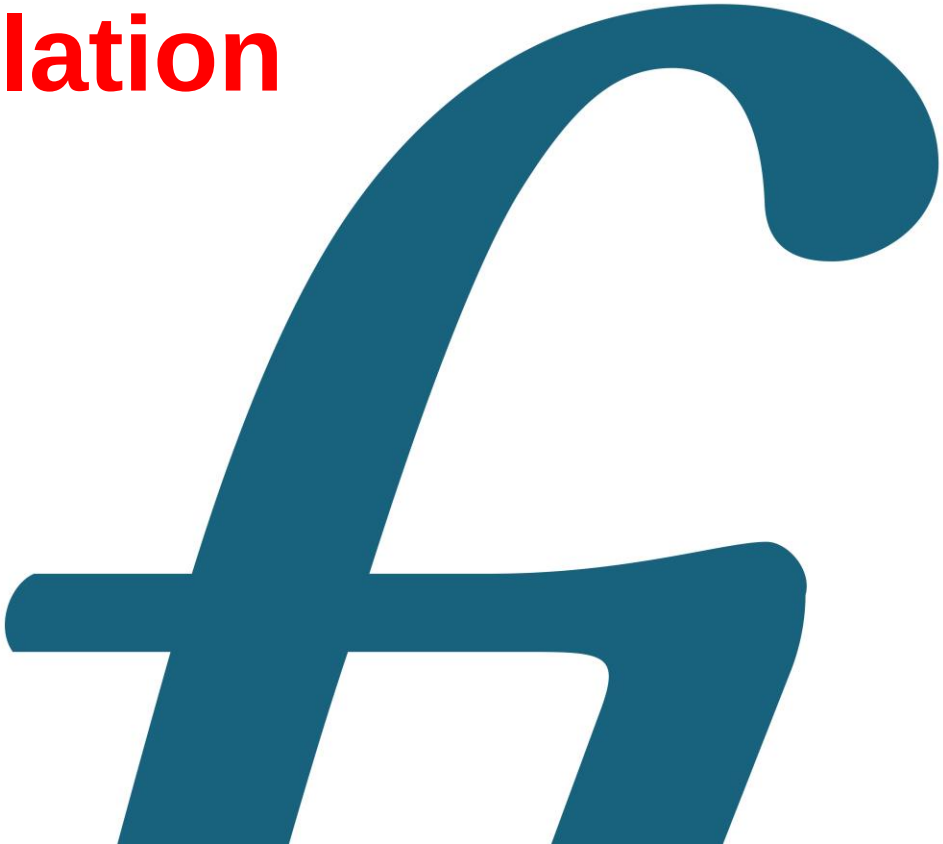
Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

GDPR – General Data Protection Regulation

Regolamento generale sulla protezione dei dati



a cura di Luciana Mellano
Bossolasco (CN) 10 Luglio 2019

Formazione IFEL
per i Comuni

Indice :

RIFERIMENTI NORMATIVI

Regolamento Ue 2016/679, noto come **GDPR** (General Data Protection Regulation) **–** relativo alla protezione delle persone fisiche con riguardo al **trattamento e alla libera circolazione dei dati personali**.

Legge di bilancio 2018 (Legge 27 dicembre 2017, n. 205, G.U. n.302 del 29-12-2017 – Suppl. Ordinario n. 62), infatti, ai commi da 1020 a 1025 dell'art. 1, ecco apparire alcune novità spiazzanti. Il comma 1020 **ci ricorda che il Garante Privacy "assicura la tutela dei diritti fondamentali e delle libertà dei cittadini"**

il comma 1021 **prevede che il Garante, con proprio provvedimento da adottare entro due mesi dalla data di entrata in vigore della legge di bilancio:**

a) disciplini le modalità attraverso le quali il Garante stesso monitora l'applicazione del regolamento GDPR e vigila sulla sua applicazione.
b) disciplini le modalità di verifica, anche attraverso l'acquisizione di informazioni dai titolari dei dati personali trattati per via automatizzata o tramite tecnologie digitali.
c) predisponga un modello di informativa da compilare a cura dei titolari di dati personali (sic) che effettuano un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati

d) definisca linee-guida o buone prassi in materia di trattamento dei dati personali fondato sull'interesse legittimo del titolare.

Il GDPR nasce da precise esigenze, come indicato dalla stessa Commissione Ue, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Ue verso altre parti del mondo. Si tratta poi di una risposta, necessarie e urgente, alle sfide poste dagli sviluppi tecnologici (i**l WP29 ha adottato tre fondamentali provvedimenti** che avranno importanti ricadute su punti essenziali del GDPR proprio sul tema dell'innovazione tecnologica) e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini Ue.

A preoccupare sono, però, le disposizioni di ratio sostanzialmente opposte che hanno attribuito agli Stati membri la possibilità di legiferare in autonomia al fine di "precisare" le norme contenute nel GDPR. In qualche modo **si è "tradita" l'iniziale visione dell'Ue** e potrebbero sorgere contrasti tra il Regolamento e le leggi nazionali adottate per allinearsi alle nuove indicazioni.

Codice Privacy (d.lgs. 196/2003) e delle altre leggi nazionali al Regolamento europeo 679/2016 sulla protezione dei dati personali (**GDPR**), adottato l'8 agosto scorso, è stato pubblicato in G.U., con il numero 101/2018 ed entrato in vigore al 19 settembre.

Uno degli aspetti più rilevanti del Decreto Legislativo 101/2018 è senz'altro quello del sistema sanzionatorio, non solo per l'evidente centralità che lo stesso riveste nel quadro della nuova normativa europea sulla protezione dei dati, ma anche perché il sistema di rinvii alle diverse disposizioni normative in esso contenute (ivi incluse quelle del d.lgs. 196/2003 che il legislatore ha scelto di non abrogare) comporta **non poche difficoltà interpretative**.

Le sanzioni amministrative GDPR

Come noto, il GDPR ha previsto **rilevanti sanzioni di natura amministrativa** in caso di violazioni della normativa sulla protezione dei dati personali.
In particolare, l'art. 83 del GDPR distingue **due gruppi di sanzioni amministrative. (pecuniarie -** suddivise per fasce di importi**)**

Le sanzioni penali GDPR

Con riguardo alle **sanzioni penali**, (illecito trattamenti) se da un lato il GDPR non ne prevede direttamente, lo stesso ammette dall'altro lato la facoltà per gli Stati membri di stabilire disposizioni relative a sanzioni penali per violazioni del GDPR, nonché violazioni di norme nazionali adottate in virtù ed entro i limiti del Regolamento (Considerando 148).

IN SINTESI CON IL GDPR :

- Si introducono regole più chiare su informativa e consenso;
- Vengono definiti i limiti al trattamento automatizzato dei dati personali;
- Poste le basi per l'esercizio di nuovi diritti;
- Stabiliti criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue;
- Fissate norme rigorose per i **casi di violazione dei dati** (**data breach**).
- Le norme si applicano anche alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti all'interno del mercato Ue. Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le nuove regole. Imprese ed enti avranno più responsabilità e caso di inosservanza delle regole rischiano pesanti sanzioni.

DEFINIZIONI :

Ai fini del regolamento s'intende per:

1)«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile;

2) «**trattamento**»: 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 registrazione, l'organizzazione, la strutturazione, 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;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «**dati relativi alla salute**»: i 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;

16) «**stabilimento principale**»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

23) «**trattamento transfrontaliero**»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

AMMINISTRATORE DI SISTEMA :

Non esiste una definizione univoca di amministratore di sistema (di seguito AdS per praticità). Il Garante in un primo approccio lo identificava in quella figura preposta alle mansioni amministrative e gestionali di reti informatiche, sistemi di sicurezza e database. Pensiamo, ad esempio**, alla gestione centralizzata delle utenze (nome utente e password), ai database dei software gestionali o che contengono dati di tipo personale** (software ERP, ad esempio) e ai sistemi di sicurezza come i firewall (che arrivano a identificare la navigazione internet o a tracciare le attività di rete provenienti da un determinato client).

Il primo grande chiarimento concernente l'amministratore di sistema viene fornito con il provvedimento 2008 del Garante Privacy, secondo il quale: "Con la definizione di *amministratore di sistema* si individuano generalmente, in ambito informatico, **figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti**.

Vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi".

LE FUNZIONI DELL' AMMINISTRATORE DI SISTEMA :

L' AdS rappresenta una figura essenziale per la sicurezza delle banche dati e la corretta gestione delle reti telematiche; è un esperto chiamato a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali; a lui viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.

E' evidente che si tratti di personale tecnico qualificato a se stante che non potrà neanche coincidere con analoghe figure di controllo quale il **Data Protection Officer** che svolge autonome attività di audit nell'ambito della sicurezza informatica.
Oltre ad essere la prima persona che dovrebbe rendersi conto di un eventuale violazione o perdita dei dati, accidentale od intenzionale che sia, è proprio l'amministratore di sistema che, con la sua attività quotidiana, svolge routine di sicurezza informatica volte a garanzia della struttura informatica (cosiddetto "data breach").

Compiti dell'amministratore di sistema:

- classificare analiticamente le banche dati e impostare/organizzare un sistema complessivo di trattamento **dei dati personali comuni e sensibili**, predisponendo e curando ogni relativa fase applicativa nel rispetto della normativa vigente in materia di protezione dei dati personali;
- individuare per iscritto **il/i soggetto/i incaricato/i della custodia delle parole chiave** per l'accesso al sistema informativo e vigilare sulla sua/loro attività;
- individuare **per iscritto gli altri soggetti**, diversi dall'/dagli incaricato/i della custodia delle parole chiave, che possono avere accesso a informazioni che concernono le medesime;
- impostare e gestire un sistema **di autenticazione informatica** per i trattamenti di dati personali effettuati con strumenti elettronici;
- impostare e gestire **un sistema di autorizzazione per gli incaricati** dei trattamenti di dati personali effettuati con strumenti elettronici;
- **adottare un sistema idoneo alla registrazione** degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo, non inferiore a sei mesi;
- **assicurare e gestire sistemi di salvataggio** e di ripristino dei dati (backup/recovery) anche automatici, nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);

- impartire **a tutti gli incaricati istruzioni** organizzative e tecniche che prevedano le modalità di utilizzo dei sistemi di salvataggio dei dati con frequenza almeno settimanale;
- adottare **procedure per la custodia delle copie di sicurezza dei dati** e per il ripristino della disponibilità dei dati e dei sistemi;
- organizzare **i flussi di rete**, la gestione dei supporti di memorizzazione, la manutenzione hardware, nonché la verifica di eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi, quali accesso abusivo al sistema informatico o telematico, frode, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici;
- predisporre **un piano di controlli periodici**, da eseguire con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate in azienda/studio professionale;
- coadiuvare, se richiesto, **il titolare del trattamento** nella predisposizione e/o nell'aggiornamento e/o nell'integrazione di tutti i documenti necessari per il rispetto del Regolamento Europeo in materia di privacy.
- Sulla base di queste considerazioni possiamo affermare che l'incarico di AdS risulta essere attuale e in linea con quanto richiesto dal Regolamento Europeo. Questa figura, infatti, è uno strumento importante sul quale il titolare del trattamento può fare affidamento per garantire che vengano rispettati i principi posti in essere dal Regolamento. È compito **dell'amministratore di sistema monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dati di cui sopra**, mantenendo aggiornati i supporti hardware e software e, se necessario, comunicando al titolare le attività da porre in essere al fine di garantire un adeguato livello di sicurezza, in proporzione alla tipologia e alla quantità dei dati personali trattati.

DATA PROTECTION OFFICER :

Cos'è il DPO, le linee guida Garanti privacy

Si conferma, inoltre, che nella disciplina estremamente succinta prevista dal legislatore europeo **il DPO è un supervisore indipendente, il quale sarà designato obbligatoriamente, da soggetti apicali di tutte le pubbliche amministrazioni e nello specifico è previsto l'obbligo nel caso in cui "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali".**

Da quanto detto sopra, emerge comunque con chiarezza che, **sebbene la designazione del Data Protection Officer sia accompagnato da una semplificazione in termini di designazione condivisa tra i diversi enti pubblici, questo adempimento comporterà certamente maggiori oneri per le finanze pubbliche.**

Il DPO in ambito privato **è obbligatorio** anche per tutte le organizzazione che trattano come attività principale **dati sensibili** (o meglio particolari secondo il regolamento) oppure dati giudiziari su larga scala, rientrano in tale previsione ospedali, assicurazioni e istituti di credito eccetera.

A seconda della complessità del contesto organizzativo in cui dovrà operare, il DPO dovrà essere anche in grado di gestire questioni inerenti le diverse giurisdizioni.

Compiti del DPO :

Più nel merito, i complessi compiti affidati al DPO sono previsti solo a livello minimale dal regolamento potendo quindi il titolare e il responsabile affidarne altri compiti, nello specifico **il Dpo dovrà**:

1) **informare e fornire** consulenza a titolare e al responsabile del trattamento nonché ai dipendenti degli obblighi derivanti dal regolamento;

2) **sorvegliare l'osservanza del regolamento**, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati;

3) **sorvegliare sulle attribuzioni** delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;

4) **fornire pareri e sorvegliare** alla redazione della Data protection impact assessment (c.d. Dpia);

5) **fungere da punto di contatto** e collaborare con l'Autorità Garante per la protezione dei dati personali;

6) **controllare che le violazioni** dei dati personali siano documentate, notificate e comunicate (c.d. Data Breach Notification Management).

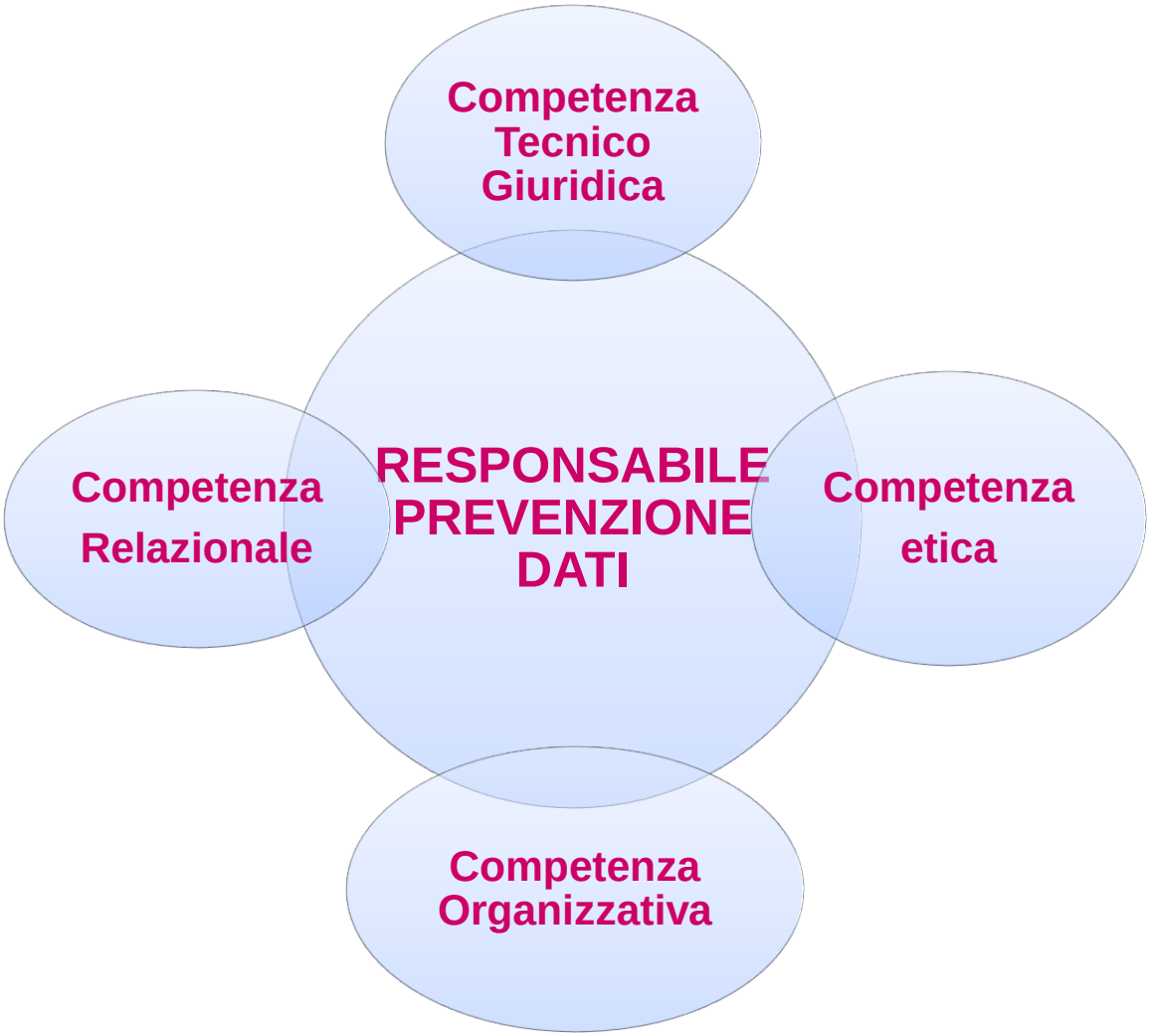
Ma come accennato il DPO potrà inoltre **gestire inventari e gestire un registro dei trattamenti e delle attività di trattamento** ex art. 30, sebbene a stretto rigore la specifica conservazione del registro della attività di trattamento ex art. 30 del regolamento europeo resti comunque ad appannaggio del titolare e del responsabile, peraltro, questi compiti sono già previsti da circa quindi anni come rientranti nel ruolo di **Data Protection Officer** interni alle istituzioni dell'Unione europea (regolamento 2001/45/Ce).

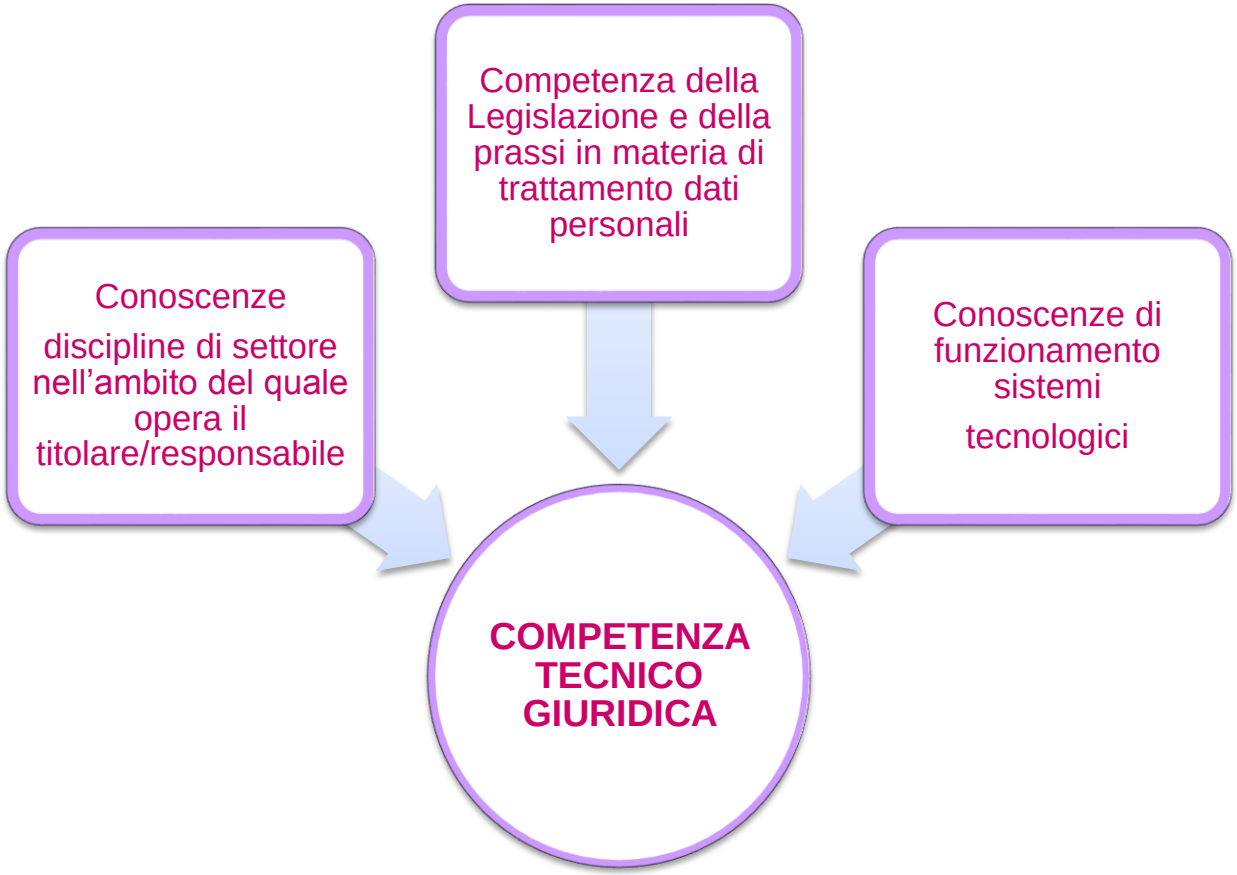
RESPONSABILE PROTEZIONE DATI :

Con l'avvento del Regolamento viene infatti introdotta, anche in Italia, una nuova figura professionale, dotata di caratteristiche peculiari, che prima non c'era e alla quale viene attribuito un ruolo chiave nell'impalcatura del sistema privacy europeo: fare da cerniera tra il titolare\responsabile del trattamento che lo ha designato, gli interessati e il Garante.
È una figura completamente diversa da quella degli altri attori del trattamento che deve essere metabolizzata e di cui non si può ancora valutare l'impatto sul sistema del trattamento dei dati personali, soprattutto nel contesto pubblico, nel quale la designazione del RPD è obbligatoria.

Si apre ora una fase nuova e complessa, in cui i Responsabili della protezione dei dati si scontreranno con la realtà e con le difficoltà legate, non solo all'interpretazione delle nuove regole e alla loro materiale applicazione nei diversi contesti ma, soprattutto, con l'affermazione del proprio ruolo nei confronti degli attori, interni ed esterni, con i quali sono chiamati a relazionarsi.

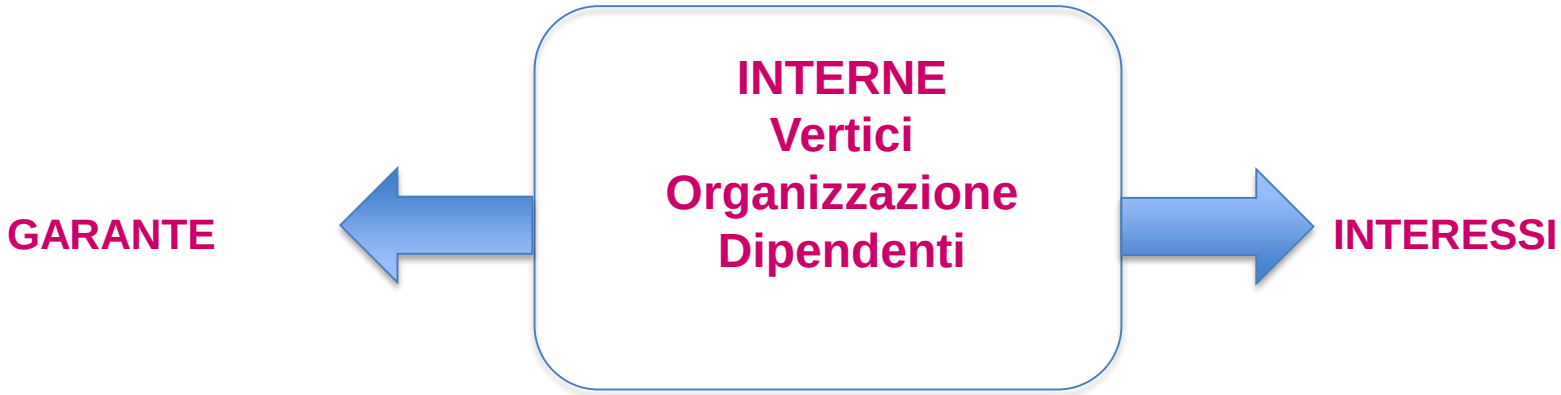
Occorre quindi avere un piano di lavoro e procedere, un passo dopo l'altro, nella direzione prestabilita, consapevoli che, **per assolvere al meglio questo importante compito, non sono sufficienti competenze tecnico-giuridiche, ma anche organizzative, relazionali ed etiche**.


Competenza Tecnico Giuridica
Competenza Relazionale
RESPONSABILE PREVENZIONE DATI
Competenza etica
Competenza Organizzativa


Competenza della Legislazione e della prassi in materia di trattamento dati personali
Conoscenze
discipline di settore nell'ambito del quale opera il titolare/responsabile
Conoscenze di funzionamento sistemi
tecnologici
COMPETENZA TECNICO GIURIDICA

LE RELAZIONI DEL RPD

ESTERNE



NEI COMUNI :

Il **Regolamento comunitario n. 2016/679** (GDPR) **non prevede** una specifica disciplina per il trattamento dei dati personali effettuato dai soggetti pubblici e quindi dai comuni. Con il presente contributo, si cerca quindi di fare il punto della situazione sul tema attraverso l'elenco dei principali obblighi che i Comuni dovranno tenere per rispettare la disciplina del GDPR entrato in vigore dal 25 maggio 2018.

Il **GDPR**, in realtà, non contiene una formale bipartizione tra titolari pubblici e privati e non contiene nemmeno norme specifiche dedicate al settore privato e pubblico, ma si occupa in generale delle condizioni di liceità del trattamento (v. **art. 6** e **art. 9, comma 2**, per i dati sensibili), anche se poi, come vedremo tra breve, alcune di esse riguardano esclusivamente lo svolgimento di attività pubbliche.

A differenza del **Codice Privacy** (**D.lgs. n. 196/2003**), il nuovo regolamento europeo non contiene la suddivisione tra condizioni di liceità applicabili a soggetti privati e condizioni valide per i soggetti pubblici, come accadeva con il Capo II del Codice Privacy, dove, ad eccezione del settore sanitario, si menzionava l'istituto del consenso quale elemento distintivo tra titolari privati e titolari pubblici.

In effetti, tra gli stessi presupposti di liceità del trattamento dei dati personali il GDPR all'**art. 6, lett. e)** fa riferimento alla necessarietà del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, caso tipico, naturalmente dell'ente pubblico.

Si pensi, poi, all'**art. 9 del GDPR** che tra le eccezioni al divieto generale di trattare dati personali sensibili fa rientrare:

- il trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento 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;
- il trattamento necessario per finalità di medicina preventiva o di medicina del lavoro,
- Il trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica;
- il trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Altra norma di sicuro interesse per l'indubbia rilevanza in materia pubblicistica è rappresentata dall'**art. 23 del GDPR** che chiarisce come il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento possa limitare, mediante specifiche misure legislative, la portata di alcuni fondamentali obblighi e diritti degli interessati qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare tra gli altri anche finalità di pubblico interesse.

Possiamo, inoltre, affermare che esistono diverse attività, svolte da soggetti pubblici, ed in particolare dai Comuni, che **non sono tecnicamente qualificabili come "compiti"**, ed è questo il caso, sottolineano i Garanti europei, dell'attività di videosorveglianza di strutture pubbliche. In questi casi, premesso che non si tratta di veri e propri compiti, c'è da domandarsi quale sia la condizione di liceità che consente ai soggetti pubblici di svolgere attività di videosorveglianza. Il gruppo dei Garanti Europei, già nell'aprile 2014, affrontò il problema con riferimento alla Direttiva 95/46/Ce, stabilendo che tale attività risultava lecita quando rispondeva ad un interesse pubblico riconducibile ai punti e) o f) dell'articolo 7 della suindicata direttiva.

Nell'ottica del GDPR se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

La responsabilizzazione dei titolari del trattamento dei dati è il principio fondamentale alla base del nuovo regolamento, mentre il secondo aspetto di rilievo riguarda la mappatura e la ricognizione dei trattamenti svolti dalle diverse amministrazioni e le loro principali caratteristiche". La ricognizione sarà l'occasione per verificare il rispetto dei principi fondamentali

Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Grazie per l'attenzione

Luciana MELLANO

E-mail : ut@comune.lombardore.to.it
Tel. 011 9956101 int. 2