Matricola n. 0000922471

ALMA MATER STUDIORUM

UNIVERSITA' DI BOLOGNA

SCUOLA DI SCIENZE

CORSO DI LAUREA IN INFORMATICA PER IL MANAGEMENT

Il trattamento dei dati personali nei Comuni Italiani

Relatore:

Chiar.ma Prof.ssa Matilde Ratti

Presentata da:

Enrico Lucarelli

Sessione II

Anno Accademico 2021/2022

Ai miei genitori,

per il dono più grande che mi hanno fatto:

il modo in cui mi hanno insegnato a vivere.

INDICE

INTRODUZIONE

Nel corso degli ultimi anni è aumentata la consapevolezza su quanto sia importante tutelare i propri dati in una società sempre più pervasa dalla tecnologia e in particolar modo da internet e dalle sue evoluzioni. Di pari passo si è evoluta ed aggiornata la normativa nell'ambito della protezione dei dati personali fino ad arrivare al Regolamento (UE) 2016/679 entrato in vigore il 25 maggio 2018. Il Regolamento, noto anche come GDPR (General Data Protection Regulation), si applica a vari contesti, pubblici e privati, che hanno fra loro strutture e finalità diverse. Tra queste vi sono i Comuni che da un lato hanno il compito di rispettare il già citato regolamento e dall'altro lato devono rispettare gli obblighi di amministrazione trasparente in capo a tutte le pubbliche amministrazioni.

Il presente elaborato si propone l'obiettivo di descrivere l'applicazione del GDPR all'interno dei Comuni italiani analizzandone le peculiarità, dettagliando le misure da mettere in campo dall'Ente e a chi sono in capo responsabilità e doveri.

Nel primo capitolo si partirà con un excursus sull'evoluzione della normativa partendo dalle sue origini fino ad arrivare al Regolamento attualmente in vigore, sottolineando in quest'ultimo l'introduzione di un principio cardine, quello dell'*accountability*. Si andranno a descrivere le definizioni e i ruoli definiti dal Regolamento in modo da conoscere a quale fattispecie si fa riferimento con determinati termini. Descritte le responsabilità assegnate ad ogni attore, si passerà alla descrizione dei principi di base per comprendere la complessa attività propedeutica alla stesura di un regolamento aderente all'attuale contesto sociale, economico e tecnologico.

Nel secondo capitolo verrà descritta la concreta applicazione del Regolamento all'interno dei Comuni italiani e ne verrà delineato l'organigramma nell'ambito della protezione dei dati personali. Particolare attenzione verrà posta sulla nuova figura introdotta dal Regolamento, quella del Responsabile della Protezione dei

dati personali. Successivamente verrà affrontato il tema della formazione, riportando a chi è in capo questa responsabilità e chi si è mobilitato per facilitare i Comuni ad adempiere a quest'obbligo. Verrà poi analizzata la valutazione d'impatto sulla protezione dei dati, quando è obbligatoria e cosa vi si trova all'interno. In ultimo verrà affrontato il tema delle sanzioni per le violazioni del Regolamento, quando vengono inflitte e fino a che cifra possono ammontare.

CAPITOLO I

IL TRATTAMENTO DEI DATI PERSONALI IN ITALIA

SOMMARIO: 1. Dalla direttiva madre alla normativa vigente – 2. Le definizioni e gli attori – 2.1 Cos'è un dato personale – 2.2 Cosa si intende per trattamento – 2.3 Titolare del trattamento – 2.4 Responsabile del trattamento 2.5 L'interessato – 2.6 Consenso dell'interessato – 3. I principi – 3.1 Liceità, correttezza e trasparenza – 3.2 Limitazione della finalità – 3.3 Minimizzazione dei dati – 3.4 Esattezza

1. Dalla direttiva madre alla normativa vigente

La prima fonte normativa nell'ambito della protezione dei dati personali a livello europeo fu la Dir. 95/46/CE, nota come Direttiva madre, del Parlamento europeo e del Consiglio del 24 ottobre 1995. La sua introduzione impose ai Paesi membri di dotarsi di una legislazione ad essa conforme, il legislatore italiano adempiette a tale obbligo nell'ultimo giorno disponibile, il 31 dicembre 1996[1]. La direttiva recepì un dibattito culturale e un pensiero dottrinale sviluppatosi nei decenni precedenti e delineò un modello statico di trattamento dei dati personali che si rivelò presto superato[2]. Bisogna precisare che all'epoca il contesto economico e tecnologico era ben diverso da quello attuale, ci riferiamo ad un mondo privo di social network e motori di ricerca, nel quale la direttiva introduceva un modello normativo che individuava un unico scambio di dati, quello dall'interessato al titolare del trattamento. Quel che social network e motori di ricerca hanno introdotto è un mondo sempre più interconnesso che non si basa più sul modello descritto prima ma su un modello

[1] La direttiva fu recepita con la Legge n. 675 del 31 dicembre del 1996.

[2] Finocchiaro, *"GDPR, perché abrogare il Codice Privacy è la scelta migliore e che cosa comporta"*, su *Agenda Digitale (www.agendadigitale.eu)*, 10 aprile 2018.

di condivisione e di cogestione di dati ed informazioni destinati, fin dall'origine, ad una circolazione globale.

La Direttiva madre, nonostante i propri obiettivi, non ha impedito la frammentazione dell'applicazione della protezione dati personali nei vari Paesi membri dell'Unione. Con la sua introduzione non si è riusciti ad eliminare l'incertezza giuridica e la percezione, largamente diffusa, che le operazioni online mettano a rischio la protezione dei dati delle persone fisiche. Per questa ragione[3] e per l'evoluzione del mondo descritta in precedenza è stato introdotto il Regolamento europeo 2016/679, applicabile dal 25 maggio 2018[4]. Trattandosi di un Regolamento, esso è direttamente applicabile in tutti gli Stati membri dell'Unione, senza la necessità di atti di recepimento nei singoli Stati.

Il legislatore italiano, negli anni precedenti, spinto anch'egli dalla volontà di rendere più chiaro il quadro normativo introdusse con il decreto legislativo n. 196 del 30 giugno 2003 il Codice in materia di protezione dei dati personali che ebbe il compito di riunificare in un unico testo le disposizioni delle varie direttive. Nel corso degli anni il testo venne prima affiancato da alcuni codici deontologici riguardanti particolari categorie di trattamento, come quello in ambito giornalistico, e poi da leggi specifiche riguardati particolari settori, come la protezione della posta elettronica. Il Codice restò la principale fonte in ambito di protezione dei dati personali fino all'introduzione del Regolamento europeo del 2018.

La principale novità dal punto di vista normativo introdotta con il GDPR fu il principio di accountability, che potremmo tradurre come principio di responsabilizzazione[5]. Fu introdotto con lo scopo di promuovere l'adozione di misure concrete e pratiche, in quanto si teorizzò che avrebbe trasformato i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del responsabile del trattamento, nel rispetto delle leggi e dei regolamenti applicabili[6]. Il responsabile del trattamento deve anche garantire

[3] Come si evince dal considerando numero 9 del Regolamento.
[4] Si tratta del Regolamento (UE) 2016/679 denominato *General Data Protection Regulation* (a cui si farà riferimento anche solo come "Regolamento" o "GDPR").
[5] Art. 5 par. 2 del Regolamento.
[6] Gruppo di lavoro ex art. 29, Parere 3/2010, 9. Il Gruppo di lavoro "Articolo 29" (Art. 29 WP) era il gruppo di lavoro europeo indipendente che, fino al 25 maggio del 2018 (entrata in vigore del RGPD) aveva lo

l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. È possibile ribadire in maniera schematica che tale disposizione si incentra su due elementi principali:

(i) la necessità che il responsabile del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati;
(ii) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile del trattamento deve fornire la prova di quanto esposto al punto (i)[7].

2. Le definizioni e gli attori

2.1 Cos'è un dato personale

La definizione di "dato personale" viene fornita all'art. 4 n. 1 del GDPR, come qualsiasi informazione riguardante una persona fisica identificata o identificabile, con un elenco esemplificativo di dati che possono rendere, direttamente ed indirettamente, identificabile la persona fisica come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Nel parere 4/2007 del gruppo di lavoro ex. Art. 29 vengono analizzati i quattro elementi fondamentali della definizione di dati personali. Con il primo, "qualsiasi informazione" risulta evidente che l'intenzione del legislatore nella stesura del Regolamento fosse quella di dare spazio ad un'ampia interpretazione del concetto a prescindere dalla natura, dal contenuto e dal formato tecnico dell'informazione. Per quanto riguarda il secondo elemento "concernente" il parere propone di avvalersi di tre distinti elementi per stabilire se le informazioni siano concernenti (ovvero se concernono) una persona e sono contenuto, finalità e risultato. Nel primo caso si fa riferimento al senso

scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali a livello europeo.
[7] *Ibidem*.

più ovvio e diffuso della parola "concernere", come sinonimo di riguardare, e di conseguenza si ha che l'elemento di "contenuto" è presente nei casi in cui l'informazione riguardante una persona è fornita a prescindere dalla finalità del responsabile del trattamento o di terzi, o dal suo impatto sulla persona interessata. Nel secondo caso l'elemento di "finalità" può essere considerato presente quando i dati sono usati al fine di valutare, trattare in un dato modo o influire sullo stato o sul comportamento di una persona. Nel terzo ed ultimo caso si ha che i dati si possono considerare "concernenti" in quanto è presente un elemento di "risultato" quando il loro impiego può avere un impatto sui diritti e sugli interessi della persona. È sufficiente che la persona sia trattata in modo diverso rispetto ad altre in seguito al trattamento dei dati.

Dato che la presente disciplina si applica alle persone fisiche identificate o identificabili, notiamo che sono quindi esclusi i dati riguardanti soggetti giuridici e che non si prende in considerazione solo l'identificazione ma anche la possibilità di un'identificazione successiva del soggetto, tramite mezzi indiretti, possibile tramite un ragionevole sforzo[8]. È evidente che siano anche esclusi dall'applicazione del Regolamento i dati anonimi, così come specificato anche al Considerando n. 26. Seppur non venga fornita una definizione analitica di dato anonimo, essa può essere comunque ricavata per sottrazione da quella di dato personale. Si considerano anonimi, dunque, quei dati che non permettono né in modo diretto né indiretto l'identificazione dell'interessato[9].

Fondamentale è la distinzione tra dato personale e informazione, evidenziata dal gruppo di lavoro ex art. 29 nel parere 4/2007. Per quanto sembrino coincidere in realtà si tratta di concetti tra loro differenti, in particolare il dato è la fonte dell'informazione, nel quale questa è contenuta e da un dato o dall'insieme di dati l'informazione può essere estratta o inferita. Quindi l'informazione non coincide con il dato stesso ma è l'elaborazione del dato[10].

[8] Cfr. Considerando n. 26 Regolamento: "si dovrebbero prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia gli sviluppi tecnologici".

[9] Cfr. Considerando n. 26 in cui il processo di identificazione viene valutato possibile sulla base dei costi, del tempo necessario, delle tecnologie disponibili al momento del trattamento e degli sviluppi tecnologici.

[10] Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Torino, 2012, 33.

2.2 Cosa si intende per trattamento

La definizione di "trattamento" viene fornita all'art. 4 n. 2 del GDPR come 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. Il Considerando n. 15 esplicita il così detto principio della neutralità tecnologica che ha il fine di garantire una effettività della tutela giuridica ed evitare l'insorgere di gravi rischi di elusione derivanti dalle tecniche e dalle tecnologie utilizzate per effettuare il trattamento. Nel Regolamento la discriminante è la finalità con la quale viene portato avanti il trattamento ed esso non si applica ai trattamenti effettuati da persone fisiche per l'esercizio di attività a carattere esclusivamente personale ed ai trattamenti effettuati da autorità giudiziarie[11].

2.3 Titolare del trattamento

Il titolare del trattamento rientra tra i così detti "soggetti attivi" ed è definito come 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[12]. La disciplina operando nell'ottica della tutela effettiva e concreta dell'interessato con il termine "determina", richiama il fatto che non sia prevista alcuna formalizzazione della titolarità del trattamento, ovvero il ruolo di titolare non viene stabilito per nomina ma da un'*influenza effettiva*[13]. Oltre allo stabilire il "come" e il "perché" delle attività di trattamento, è in campo al titolare del trattamento il rispetto per paragrafo 1 dell'art. 5 del Regolamento e la possibilità di comprovare tale rispetto[14].

[11] Art. 2 n. 2 comma c) e d) Regolamento.
[12] Art. 4 par. 1 n. 7 Regolamento.
[13] Gruppo di lavoro ex art. 29, Parere 1/2010 (WP169), 11.
[14] Art. 5 n. 2 Regolamento.

2.4 Responsabile del trattamento

Anche il responsabile del trattamento rientra tra i "soggetti attivi" ed è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento[15]. Come si evince, il responsabile ha un ruolo subordinato al titolare e viene designato tramite una nomina nella quale vengono indicate le istruzioni per trattare i dati per conto del titolare[16]. Il questa maniera il Legislatore ha previsto che il responsabile del trattamento possa godere di una cera discrezionalità ma limitatamente di tipo tecnico-professionale in quanto, se quest'ultimo dovesse andare oltre le istruzioni fornitegli tramite nomina e acquisisse un ruolo determinante nella decisione di finalità e mezzi di trattamento esso diventerebbe, di fatto un titolare o un contitolare del trattamento[17].

2.5 L'interessato

Visti i soggetti attivi passiamo al soggetto passivo: l'interessato. Esso è il soggetto principale della disciplina ed è definito come la persona fisica identificata o identificabile alla quale riferiscono i dati personali. Elemento di incertezza e meritevole di approfondimento è il concetto di persona fisica "identificabile". Il Legislatore per dissipare dubbi ed incertezze all'art. 4 del Regolamento fornisce un elenco esemplificativo di elementi che rientrano sotto la definizione di identificativo. L'elemento chiarificato lo troviamo però nel Considerando 26 che recita "Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente.". Quello che evince è che l'identificabilità di una persona va valutata caso per caso a seconda dei mezzi a disposizione del titolare per l'identificazione dell'interessato.

[15] Art. 4 par. 1 n. 8 Regolamento.
[16] Art. 28 n. 3 Regolamento.
[17] Gruppo di lavoro ex art. 29, Parere 1/2010, 26.

2.6 Consenso dell'interessato

Al numero 1 dell'articolo 6 del Regolamento troviamo che il consenso è una delle condizioni che rendono lecito il trattamento dei dati. Per i trattamenti la cui liceità è basata sul consenso è fondamentale che esso sia valido. Per esserlo il consenso espresso dall'interessato deve essere dimostrabile, specifico, chiaro, revocabile ed informato[18].

3. I principi

Nell'art. 5, intitolato "Principi applicabili al trattamento dei dati personali" troviamo un elenco di disposizioni generali contenenti principi applicabili ad ogni aspetto della disciplina in oggetto.

3.1 Liceità, correttezza e trasparenza

Al paragrafo uno dell'art. 5 del Regolamento troviamo un elenco di principi generali, il primo di essi di divide in tre sotto-principi: liceità, correttezza e trasparenza. Ponendo l'attenzione sul primo di essi notiamo che è presente anche nel successivo art. 6 del Regolamento[19]. Non si tratta di una ripetizione superflua ma caratterizza due diversi fini delle disposizioni, la prima previsione determina il collegamento sistematico rispetto a fonti diversamente collocate nell'ordinamento giuridico, la seconda, invece, specifica i presupposti che rendono lecito un trattamento. Attuando un'interpretazione in combinato disposto delle due norme, si configura una procedura che si compone di due momenti. In un primo momento l'interprete dovrà verificare che il trattamento sia conforme ad una delle condizioni di liceità ex art. 6 del Regolamento, superata con successo questa fase nel secondo momento verrà valutato se il trattamento sia "conforme al diritto" e, dunque, se dal trattamento non derivi

[18] Art. 7 del Reg. rubricato "Condizioni del consenso".
[19] Art. 6 del Reg. rubricato "Liceità del trattamento".

alcuna lesione degli interessi e dei valori protetti dall'ordinamento[20]. Il principio di liceità, pertanto, funge da collegamento tra la norma di settore e l'insieme delle disposizioni dell'ordinamento giuridico che proteggono a loro volta ulteriori interessi meritevoli di tutela[21]. Il secondo sotto-principio è quello della correttezza e richiama la nozione civilistica di buona fede e correttezza, principi già noti in materia di contratti e obbligazioni. Il terzo ed ultimo sotto-principio è quello di trasparenza, introdotto con il Regolamento in quanto non presente nella precedente Dir. 95/46/CE. Tale principio si configura come espressione del diritto di accesso ai dati personali come si può evincere anche dal considerando 39 che recita "*Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.*".

3.2 Limitazione della finalità

Alla lettera b) dell'articolo in esame, troviamo il principio della limitazione della finalità che comporta l'esclusione di repentini cambiamenti nelle condizioni fondamentali del trattamento garantendo che i dati personali vengano raccolti e trattati per le finalità previste a priori, immediatamente rese note all'interessato e in conformità con l'ordinamento giuridico di riferimento. Per i trattamenti successivi si dispone un vincolo del trattamento alle medesime finalità. Tuttavia, riguardo quest'ultima disposizione, sono stati introdotti dei temperamenti al fine di evitare una tutela inadeguata all'utilizzo degli strumenti tecnologici. Conscio del rischio di una disciplina anacronisticamente distante dalla realtà, il Legislatore europeo ha introdotto, all'art. 6 par. 4 del testo in commento, una serie di indici volti a mitigare il rigore della previsione centrale ed a verificare se il trattamento per un'altra finalità possa essere, nel caso di specie, compatibile con la finalità iniziale. Nello specifico: l'esistenza di un nesso tra la finalità iniziale e quella successiva, l'analisi del contesto, della

[20] Bravo, *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in Finocchiaro (diretto da), op. cit., 111-123.
[21] P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. Pardolesi (a cura di), 2003, *Diritto alla riservatezza e circolazione dei dati personali*, I, Giuffrè, Milano, 415.

natura dei dati o delle possibili conseguenze per l'interessato dal trattamento ulteriore, nonché, l'applicazione di garanzie adeguate, quali la cifratura o la pseudonimizzazione, sia nel trattamento originario che in quello successivo. Ulteriori attenuazioni vengono riportate nel Considerando 50 nel quale è specificato che il titolare del trattamento possa prescindere dalla compatibilità delle finalità in caso di consenso dell'interessato ovvero qualora il trattamento, per il diritto dell'Unione o degli Stati membri, costituisca una misura necessaria e proporzionata finalizzata alla salvaguardia di importanti obiettivi di interesse pubblico generale. Inoltre, lo stesso art. 5 nella sua parte conclusiva, legittima i trattamenti successivi non compatibili con quelli antecedenti, qualora vengano effettuati per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

3.3 Minimizzazione dei dati

Alla lettera c) del medesimo articolo troviamo il principio di minimizzazione dei dati che ha come fine quello di impedire trattamenti inutili e potenzialmente illeciti[22]. La norma prevede che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. A tal proposito nel Considerando 39 viene chiarito che il trattamento dei dati debba avvenire soltanto in condizioni di necessarietà da cui consegue, sulla base della stessa ragione, un tempo di conservazione dei dati limitato al raggiungimento dello scopo così come l'utilizzo degli stessi relegato all' eventualità in cui la finalità della relativa operazione non possa essere raggiunta con alti mezzi.

3.4 Esattezza

Per ultimo analizziamo il principio dell'esattezza che si trova alla lett. d) dell'art. 5. Questo principio dispone che i dati siano esatti e, se necessario, aggiornati. A tal proposito il Considerando 39 recita che "È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati.". Ciò che si evince in conclusione è che il principio di esattezza

[22] Gruppo di lavoro ex art. 29, Parere 2/2013, 17.

riguarda la qualità dei dati personali, l'insieme dei diritti dell'interessato che ne derivano e allo stesso tempo gli obblighi per il titolare che effettua il trattamento, che si concretizzano nella cancellazione[23] e la rettifica[24] dei dati stessi.

[23] Diritto previsto dall'art. 17 del Regolamento.
[24] Diritto previsto dall'art. 16 del Regolamento.

CAPITOLO II

L'APPLICAZIONE DEL REGOLAMENTO NEI COMUNI ITALIANI

SOMMARIO: 1. L'organigramma nei Comuni e il "titolare diffuso" – 1.1 Il Comune quale titolare del trattamento – 1.2 Il Responsabile del trattamento nel Comune – 1.3 Gli incaricati nel Comune – 1.4 Il Responsabile della protezione dei dati – 2. La formazione – 2.1 Il ruolo del RPD sulla formazione – 2.2 Laboratorio Privacy, formazione e software – 2.3 Il progetto T4DATA – 3. La valutazione d'impatto sulla protezione dei dati – 4. La violazione dei dati personali – 4.1 I comportamenti da adottare – 4.2 Le sanzioni

1. L'organigramma nei Comuni e il "titolare diffuso"

Date le definizioni dei vari ruoli nel capitolo precedente ora andiamo a vedere quali figure li ricoprono all'interno dei Comuni. C'è da precisare che l'organizzazione potrebbe subire alcune variazioni a seconda della dimensione dell'ente come vedremo più avanti. In questa fase è però importante ricordare che i piccoli Comuni[25] rappresentano circa il 70% dei Comuni italiani[26].

1.1 Il Comune quale titolare del trattamento

Nell'ambito dei Comuni il ruolo il ruolo di titolare del trattamento è in capo all'ente stesso[27] e le funzioni ad esso attribuite dal ruolo vengono esercitate dal Sindaco che determinerà le finalità ed i mezzi del trattamento. Approfondendo la figura del titolare del trattamento si nota come, oltre a determinare finalità e mezzi del trattamento, questi abbia molte altre competenze tra le quali: in caso di minori, verifica che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale (art. 9); agevola l'esercizio dei diritti dell'interessato (art. 12) e

[25] Con "piccoli Comuni" si afferisce ai Comuni sotto ai 5.000 abitanti.
[26] Fonte ISTAT, dato al 1/01/2022.
[27] "Quando la raccolta, l'elaborazione, l'utilizzazione, la conservazione e in genere tutte le operazioni relative al trattamento dei dati vengono effettuate nell'ambito di un'amministrazione pubblica, di una società o di un ente, il titolare del trattamento è la struttura nel suo complesso e cioè il soggetto al quale competono le scelte di fondo sulla raccolta e sull'utilizzazione dei dati." Comunicato stampa del Garante, in Bollettino, 1997.

fornisce agli interessati le informazioni indicate dal GDPR (art. 13); mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento (principio di accountability art. 24); individua i responsabili del trattamento e ne controlla e garantisce l'operato (art.28); tiene un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30); garantisce l'idoneità formazione del personale incaricato del trattamento (art. 32), comunica all'autorità di controllo (art. 33) e all'interessato (art. 34) eventuali violazioni dei dati; effettua: prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35); designa il responsabile della protezione dei dati (art. 37) mettendolo in grado di svolgere adeguatamente l'attività (art. 38); è destinatario di provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58); risponde per il danno cagionato dal suo trattamento che violi il presente regolamento (art. 82); è destinatario delle sanzioni amministrative pecuniarie inflitte ai sensi del GDPR (art. 83). Da questo elenco di competenze, principali ma non esclusive, del Sindaco, è evidente che esse devono trovare una collocazione organizzativa adeguata a garantire la regola aurea della competenza: allocazione della responsabilità giuridica (deve decidere chi ha formalmente il potere di farlo) e riconoscimento delle professionalità (deve fare le cose chi sa farle)[28]. L'idea di fondo è che la logica della responsabilizzazione, che permea il GDPR, debba partire dalla consapevolezza della complessità della figura del titolare del trattamento e della necessità conseguente di adottare un modello organizzativo di tipo composito che viene definito del "titolare diffuso"[29][30].

[28] Tirabassi, *L'attuazione del GDPR. Un modello organizzativo per gli enti locali*, 2018, 990.
[29] *Ibidem*, 989.
[30] Soffermandoci su questo aspetto possiamo notare come questa modalità organizzativa è già utilizzata dai Comuni per altre funzioni. Riporto l'esempio della realizzazione di un'opera pubblica, in cui il consiglio comunale approva bilancio e il piano delle opere, l'organo esecutivo (la giunta comunale) delibera il progetto, i dirigenti definiscono le procedure di affidamento, ma questa ripartizione della competenza articola e convive con la piena titolarità dell'opera in capo al Comune.

1.2 Il Responsabile del trattamento nel Comune

Il Responsabile del trattamento è, come si è detto in precedenza, quella figura designata dal titolare del trattamento al fine di trattare i dati per suo conto e nei limiti e nelle modalità da lui indicate[31]. Nei Comuni questo ruolo viene ricoperto da uno o più dirigenti/responsabili di unità operative a seconda della grandezza dell'ente[32]. Questo vale per i trattamenti svolti all'interno dell'ente dove i dirigenti sono responsabili dei trattamenti avvenuti nelle loro aree. Se prendiamo invece il caso di una società partecipata che offre servizi per la gestione delle entrate comunali è evidente che la società dovrà disporre dei dati personali dei contribuenti. In questo caso la titolarità del trattamento resta in capo al Comune, mentre la responsabilità del trattamento sarà in capo alla società stessa[33].

1.3 Gli incaricati nel Comune

La figura dell'incaricato era indicata all'art. 4 del Codice privacy poi abrogato (con l'introduzione del Regolamento), ma si tratta di un aggiornamento terminologico, cioè scompare la figura ma nei fatti rimane come <<persona autorizzata>>[34]. Nell'ambito comunale essi sono i dipendenti che vengono autorizzati dai relativi capi area nel ruolo di responsabili del trattamento. In maniera speculare nell'esempio della società partecipata saranno i dipendenti della società stessa.

1.4 Il Responsabile della protezione dei dati

Il Responsabile della protezione dei dati (anche solo RPD) è obbligatorio per gli enti pubblici[35]. Al RPD sono assegnati vari compiti tra i quali: informare e fornire consulenza al titolare del trattamento o del responsabile del trattamento nonché ai

[31] Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, 3.
[32] Quaderno ANCI, *L'attuazione negli Enti Locali del nuovo Regolamento UE n. 679/2016 sulla protezione dei dati personali*, 2018, 7.
[33] Braccini, *Privacy e dati personali: cosa cambia con l'arrivo delle nuove regole europee per gli enti locali*, in *Aziendaitalia*, 2018, pp. 435 e ss.
[34] *La Protezione dei Dati Personali in Italia*, diretto da Finocchiaro, 100, Pizzetti, P*rivacy e il diritto eurpeo*, 1, cit., 205-206
[35] Art. 37 n. 1 lett. a.

dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; sorvegliare l'osservanza del Regolamento, nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fornire, se richiesto, un parere in merito alla valutazione d'impatto dei dati e sorvegliarne lo svolgimento; cooperare con l'autorità di controllo; fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione[36].

Per l'individuazione il Regolamento non prevede una selezione per titoli che potrebbe apparire sproporzionata e discriminatoria, tenuto conto che tali requisiti, di per sé, non sono necessariamente in grado di dimostrare il possesso delle competenze tecniche per lo svolgimento adeguato della funzione di RPD[37]. Il Regolamento prevede invece che venga selezionato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e delle capacità di assolvere i suoi compiti[38]. Il ruolo può essere ricoperto sia da un soggetto interno all'ente sia da un soggetto esterno. Nel caso di un soggetto interno con già un incarico dirigenziale all'interno dell'ente ciò non dovrebbe comportare la sottrazione del tempo necessario allo svolgimento dei compiti assegnati al RPD, né dovrebbe dare luogo a una situazione di conflitti di interessi qualora ad esempio partecipi alla definizione delle finalità o modalità di trattamento dei dati personali effettuati dal titolare[39]. In caso di designazione di un soggetto esterno l'ente potrebbe nominare direttamente una persona fisica oppure una persona giuridica. Nel caso della persona giuridica essa è tenuta ad individuare il referente persona fisica e è opportuno che essa sia indicata già in fase di procedura di selezione[40]. C'è

[36] Art. 39 n. 1 Regolamento.
[37] Garante per la protezione dei dati personali, *Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*, 2021, 14.
[38] Art. 37 n. 5 Regolamento.
[39] Garante per la protezione dei dati personali, *Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*, 2021, 10.
[40] *Ibidem*, 18

un'ulteriore possibilità per i Comuni di piccole dimensioni, quella di indicare un RPD esterno condiviso con altri enti[41]. Lo svolgimento della funzione di RPD per conto di più titolari deve necessariamente tenere conto della possibilità di consentire, alla figura incaricata, di prestare il necessario supporto a tutti i suddetti titolari (anche in termini di tempo e disponibilità da dedicare loro) e di assolvere in maniera adeguata ai suoi compiti[42].

2. La formazione

Come abbiamo visto nel caso del Responsabile per la Protezione dei dati personali è molto importante la competenza e quindi la formazione. Questo principio non vale solo il RPD ma anche dei soggetti incaricati a effettuare un trattamento per conto del Titolare. A tal proposito l'art. 29 del Regolamento recita: "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*".

2.1 Il ruolo del RPD sulla formazione

Nell'ambito della formazione un ruolo importante è ricoperto dal Responsabile della Protezione dei dati che ha il compito di sorvegliare sulla sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo[43]. Dato che il Regolamento non stabilisce le forme in cui la formazione debba avvenire, potrebbe essere lo stesso RPD, su espresso mandato del Titolare del trattamento, a tenere giornate formative per i dipendenti dell'ente date le sue indubbie competenze derivanti dal ruolo che riveste.

---

[41] Art. 37 n. 3 Regolamento.
[42] Garante per la protezione dei dati personali, *Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*, 2021, 11.
[43] Art. 39 lett. b Regolamento.

2.2 Laboratorio Privacy, formazione e software

Sempre nell'ambito della formazione del personale, finalizzata a mettere in campo pratiche di trattamento dei dati nel rispetto del Regolamento, è intervenuta anche l'Associazione Nazione Comuni Italiani (ANCI). Lo ha fatto tramite un progetto dell'Anci Digitale[44] denominato "*Laboratorio Privacy*". Il servizio di Anci Digitale sulla privacy, dedicato ai comuni italiani, è costituito da un software specializzato nella gestione degli adempimenti previsti dal Regolamento supportato da un'attività di formazione attraverso webinar e attività di consulenza per la predisposizione del Registro dei Trattamenti e relativo Piano di Miglioramento (*remediation plan*). Anci Digitale affianca i Comuni italiani nella formazione specialistica sul Regolamento per la protezione dei dati personali e lo fa con un programma formativo ideato specificamente per gli enti locali. I punti del programma sono: le basi della privacy; il nuovo principio di *accountability*; privacy e sicurezza informatica – la protezione dei dati personali fra d.lgs. 196/2003 e regolamento 679/2016; il registro dei trattamenti; analisi dei rischi e misure di sicurezza; i ruoli e le figure privacy – il titolare del trattamento, il responsabile del trattamento e l'interessato; le informative verso il cittadino, il consenso; la protezione dei dati personali fra d.lgs. 196/2003 e GDPR 679/2016; principi della sicurezza informatica; DPIA (Valutazione d'Impatto della Proteazione dei Dati); il ruolo del responsabile della protezione dei dati; come gestire il "sistema privacy" comunale[45]. Anci Digitale offre anche la figura del DPO esterno per l'ente che andrebbe nominato come descritto nei paragrafi precedenti.

[44] Anci Digitale S.p.A società in house dell'Associazione Nazionale Comuni Italiani e Aci Informatica per la creazione di servizi informativi, banche dati e servizi telematici destinati al sistema delle Autonomie Locali e dei Comuni in particolare.

[45] Sito Anci Digitale, https://www.ancidigitale.it/portfolio-articoli/elp-enti-locali-e-privacy/

2.3 Il progetto T4DATA

Anche il Garante per la protezione dei dati personali si è attivato per la formazione e la divulgazione delle giuste pratiche e lo ha fatto nel ruolo di promotore del progetto T4DATA (ossia "Training For Data"). Il progetto, che si svolto nel biennio 2018-2019, prevede una serie di attività transnazionali di formazione dei formatori (realizzate nel 2018) e, a livello nazionale, numerose iniziative formative gratuite dedicate ai Responsabili della Protezione dei Dati operanti presso i soggetti pubblici, tra cui un ciclo di seminari in varie città d'Italia, un manuale e una vasta offerta di webinar tenuti da esperti giuristi e funzionari e dirigenti del Garante e dedicati ad approfondire numerosi temi del Regolamento e della disciplina nazionale in materia di protezione dei dati personali. Finanziato con i fondi del Rights, Equality and Citizenship Programme dell'Unione europea (2014-2020), T4DATA ha coinvolto le autorità per la protezione dati di 5 Paesi Ue - Bulgaria, Croazia, Italia, Polonia e Spagna – oltre alla fondazione Elio e Lisli Basso[46].

I webinar realizzati per il progetto sono disponibili su una piattaforma appositamente progettata per la formazione e-learning - sviluppata *ad hoc* grazie alla collaborazione, per la parte tecnologica, del Politecnico di Milano - che presenta oltre 30 webinar, articolati in 4 moduli principali: I fondamentali della protezione dei dati, Il Responsabile della Protezione dei Dati, Il toolkit del RPD e Approfondimenti. Gli utenti sono liberi di selezionare il percorso più adatto alle proprie esigenze. All'interno della piattaforma oltre ai webinar sono messe a disposizione slides presentate dai docenti, eventuali materiali di approfondimento e un test di auto-valutazione per valutare autonomamente la comprensione dei contenuti[47].

In Italia sono stati svolti quattro seminari, nelle città di Torino, Ancora, Roma e Catanzaro, che hanno raccolto la partecipazione di oltre 1.300 Responsabili della Protezione dei Dati presso soggetti pubblici. Un dato per il quale è lecito affermare che il bilancio dell'attività di formazione sul territorio legata al progetto T4DATA è assolutamente positivo. In ognuno di questo di questi seminari è stato affrontato

[46] Sito ufficiale del progetto T4DATA, https://www.garanteprivacy.it/regolamentoue/formazione/t4data
[47] *Ibidem*.

uno specifico tema, a Torino "La gestione del rischio e la sicurezza del trattamento", a Roma "Le responsabilità del trattamento", a Catanzaro "Protezione dei dati personali e trasparenza della PA dopo il Regolamento (UE) 2016/679" e ad Ancona "Il trattamento dei dati personali per finalità di cura e ricerca", con interventi di dirigenti e funzionari del Garante[48].

3. La valutazione d'impatto sulla protezione dei dati

Un altro elemento introdotto dal Regolamento è la valutazione d'impatto sulla protezione dei dati (DPIA[49]) che il titolare del trattamento deve effettuare prima di procede al trattamento quando esso può presentare un rischio elevato per i diritti e le libertà delle persone fisiche[50] ed in particolare nei seguenti casi: una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati; la sorveglianza sistematica su larga scala di una zona accessibile al pubblico[51].

La valutazione deve contenere almeno: una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una valutazione dei rischi per i diritti e libertà degli interessati; le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alla presente regolamento,

[48] Comunicato Stampa del Garante, "GDPR: bilancio positivo per il progetto formativo internazionale T4DATA. Oltre alle iniziative sul territorio, lanciata una piattaforma di e-learning".
[49] Acronimo di *Data Protection Impact Assessment.*
[50] Art. 35 n. 1 del Regolamento.
[51] Art. 35 n. 3 del Regolamento.

tenuto conto dei diritti e degli interessi degli interessati e delle altre persone in questione[52].

La DPIA è uno strumento fondamentale in quanto oltre ad aiutare il titolare del trattamento a rispettare le prescrizioni del Regolamento, gli permette anche di realizzare il principio di responsabilizzazione ed attestare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni[53].

Data questa doppia valenza, tutti i Comuni dovrebbero effettuare una DPIA, anche i più piccoli dove il titolare non riscontra un elevato rischio nel trattamento dei dati, proprio perché lo aiuterebbe a rispettare il principio di accountability. Un ulteriore incentivo potrebbe essere il fatto che il Regolamento prevede di poter effettuare una DPIA non su un unico progetto ma per esempio su più autorità pubbliche o enti pubblici che intendono istituire un'applicazione o una piattaforma di trattamento comuni[54]. Potrebbe essere il caso dei Comuni che decidono di utilizzare il software realizzato da Anci Digitale.

4. La violazione dei dati personali

Con violazione dei dati personali (o "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati[55].

4.1 I comportamenti da adottare

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei

[52] Art. 35 n. 7 del Regolamento.
[53] Braccini, *Privacy e dati personali: cosa cambia con l'arrivo delle nuove regole europee per gli enti locali*, 2018.
[54] Considerando n. 92.
[55] Art. 4 par. 1 n. 12 del Regolamento.

loro diritti, discriminazione, furto o usurpazione d'identità o qualsiasi altro danno economico o sociale significativo alla persona interessata. Per questo motivo, il titolare del trattamento (nel nostro caso l'ente locale, il quale agisce tramite il Sindaco) non appena venuto a conoscenza di una violazione dei dati dovrebbe valutare se questa violazione presenti dei rischi per i diritti e le libertà delle persone fisiche coinvolte. Nel caso ritenga che questo rischio sia presenta dovrà notificare la violazione all'autorità competente[56], senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Nel caso ritenga che non vi sia rischio dovrà essere in grado di dimostrarlo nel rispetto del principio di *accountability*. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo[57]. Il responsabile del trattamento (se ce ne sono più di uno, quello sotto il quale avviene la violazione) informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. La notifica da inviare all'autorità competente deve contenere almeno: descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; descrivere le probabili conseguenze della violazione dei dati personali; descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi[58].

[56] In Italia l'autorità di controllo è l'Autorità Garante per la Protezione dei Dati Personali.
[57] Considerando 85.
[58] Art. 33 par 2, 3 del Regolamento.

4.2 Le sanzioni

Il Regolamento prevede che ogni autorità di controllo provveda affinché le sanzioni amministrative pecuniarie inflitte, ai sensi dell'articolo 83, siano in ogni caso effettive, proporzionate e dissuasive[59]. Al momento della decisione dell'inflizione di una sanzione e al fissare dell'ammontare della stessa in ogni singolo caso va tenuto conto dei seguenti: la natura, la gravità e la durata della violazione nonché il numero di interessati lesi; il carattere doloso o colposo della violazione; le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno dagli interessati; il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche organizzative da essi messe in atto; eventuali precedenti violazioni commesse dal titolare del trattamento o dal responsabile del trattamento; il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; e categorie di dati personali interessate dalla violazione; a maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; qualora siano stati precedentemente disposti provvedimenti, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione[60].

Le sanzioni amministrative pecuniarie hanno due tetti massimi a seconda delle disposizioni che vengono violate. Possono arrivare fino a 10 000 000 €, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, se riguardano gli obblighi del titolare del trattamento e del responsabile del trattamento, gli obblighi dell'organismo di certificazione o gli obblighi dell'organismo di controllo[61]. Il tetto massimo sale a 20 000 000 €, o per

[59] Art. 83 n. 1 del Regolamento.
[60] Art. 83 n.2 Regolamento.
[61] Art. 83 n. 4 del Regolamento.

le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, se le violazioni riguardano i principi di base del trattamento, le condizioni relative al consenso, i diritti dell'interessato, i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale, qualsiasi obbligo ai sensi delle legislazioni degli Stati membri, l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo[62].

[62] Art. 83 n. 5 del Regolamento.

CONCLUSIONI

Ripercorrendo l'analisi condotta è possibile trarre alcune conclusioni.

Innanzitutto le differenze nell'applicazione del Regolamento da parte di soggetti privati ed enti pubblici, nel nostro caso i Comuni. In primis la figura del Responsabile della protezione dei dati che sempre obbligatoria per gli enti pubblici e che per i soggetti privati lo diventa solo in caso in cui essi svolgono trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure riguardano, su larga scala, categorie particolari di dati personali di cui agli articoli 9 e 10 del Regolamento.

Un'altra differenza tra i due settori è il livello di formazione e specializzazione del personale. È noto come gli enti pubblici debbano rispettare stringenti normative in ambito di assunzione del personale a cui i privati non sono sottoposti. Proprio per queste differenze nella libertà di selezione e assunzione del personale nelle strutture private è più probabile che sia stato individuato un RPD interno rispetto alle strutture pubbliche dove, per mancanza di competenze interne, si predilige individuare una figura esterna.

Da questa disparità viene evidenziata l'importanza di un altro fattore analizzato nell'elaborato che è quello della formazione del personale nei Comuni italiani. In questo ambito forte rilievo hanno avuto i progetti citati tra i quali il progetto T4DATA che, anche alla luce dei dati di partecipazione riportati, non può che avere una valutazione positiva sia dal punto di vista della sensibilizzazione che dell'interiorizzazione della normativa all'interno del Regolamento.

BIBLIOGRAFIA

Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Torino, 2012.

Finocchiaro (diretto da), *La protezione dei dati in Italia Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, vol. I, Giuffrè, 2003.

Braccini, *Privacy e dati personali: cosa cambia con l'arrivo delle nuove regole europee per gli enti locali*, in *Aziendaitalia*, 2018, pp. 435 e ss.

Finocchiaro, *"GDPR, perché abrogare il Codice Privacy è la scelta migliore e che cosa comporta"*, su *Agenda Digitale (www.agendadigitale.eu)*, 10 aprile 2018

Tirabassi*, L'attuazione del GDPR. Un modello organizzativo per gli enti locali*, in *Aziendaitalia*, 2018, pp. 988 e ss.

STRUMENTI ESEGETICI

Gruppo di lavoro ex art. 29, *Parere 3/2010 sul principio di responsabilità*, (WP173)

Gruppo di lavoro ex art. 29, *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, (WP169)

Gruppo di lavoro ex art. 29, *Parere 2/2013 sulle applicazioni per dispositivi intelligenti*, (WP202)

SITOGRAFIA

Finocchiaro, *"GDPR, perché abrogare il Codice Privacy è la scelta migliore e che cosa comporta"* https://www.agendadigitale.eu/sicurezza/privacy/gdpr-perche-abrogare-il-codice-privacy-e-la-scelta-migliore-e-che-cosa-comporta/

Sito Anci Digitale, https://www.ancidigitale.it/portfolio-articoli/elp-enti-locali-e-privacy/

Sito ufficiale del progetto T4DATA, https://www.garanteprivacy.it/regolamentoue/formazione/t4data

Comunicato Stampa del Garante, "GDPR: bilancio positivo per il progetto formativo internazionale T4DATA. Oltre alle iniziative sul territorio, lanciata una piattaforma di e-learning". https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9201127