COMUNE DI TRESIGNANA

MODELLO ORGANIZZATIVO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

Approvato con deliberazione della Giunta comunale n. 70 del 18-09-2024

INDICE

GLOSSARIO

RGDP/GDPR = Regolamento Generale sulla Protezione dei Dati Personali, Regolamento 2016/679/UE;

RPD/DPO = Responsabile della protezione dei dati (in inglese DPO - *Data Protection Officer*);

Data breach = "riuscire a fare breccia", qualunque violazione dei dati personali;

DPIA = Valutazione di impatto sulla protezione dei dati;

Privacy by design = Privacy dal momento della sua progettazione. Implica che qualsiasi progetto va realizzato assumendo dalla fase iniziale di ideazione misure di protezione di dati personali;

Privacy by default = protezione dei dati per impostazione predefinita, ovvero, misure tecniche e organizzative che assicurano solo i dati personali necessari per ogni specifica finalità di trattamento;

Audit Privacy = è una valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Regolamento 2016/679/UE;

GEPD = Garante europeo della protezione dei dati;

Accountability = letteralmente "rendere conto", ovvero, il titolare del trattamento si deve responsabilizzare autonomamente nella gestione e organizzazione della tutela dei dati personali e, più in generale, della *privacy*. Il principio nasce nella legislazione europea e statunitense ed è inteso come la responsabilità dell'amministrazione ha verso chi l'ha scelta e si fonda su: trasparenza intesa come informazioni dell'attività di governo; partecipazione di chiunque al miglioramento delle politiche pubbliche e collaborazione intesa come efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo;

WP 29 = *Warking Party* Art. 29 (c.d. Gruppo di lavoro art. 29) - Organismo consultivo e indipendente composto da un rappresentante dei Garanti dei dati personali di ogni stato membro, da un rappresentante della Commissione UE e dal Garante europeo della protezione dei dati.

PREMESSA

Il 25 maggio 2018 è divenuto ufficialmente operativo il nuovo Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Il GDPR, acronimo di *General Data Protection Regulation* va ad abrogare, dopo oltre un ventennio, la cosiddetta direttiva 'madre' 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che, fino ad oggi, costituiva il quadro normativo di riferimento a livello europeo. Il nuovo Regolamento costituisce, insieme alla direttiva 2016/680/UE, il "Pacchetto di protezione dei dati" elaborato e approvato dall'Unione Europea.

Il Regolamento 2016/679/UE del Parlamento europeo e del Consiglio del 27 aprile 2016 fa riferimento a dati concernenti persone identificate o identificabili in possesso di vari soggetti e quindi anche della pubblica amministrazione, utilizzabili per le proprie finalità istituzionali. Dati che devono essere trattati nei limiti delle funzioni dell'ente, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.

Il nuovo apparato normativo si regge su di un nuovo principio di fondamentale importanza: la responsabilizzazione, ovvero il principio di *accountability* (nell'accezione inglese).

Tale concetto rappresenta un'assoluta novità nel campo della protezione dei dati personali, in quanto il titolare del trattamento, oltre ad avere l'esclusiva competenza per il rispetto dei principi e delle regole previste dal Regolamento, deve anche essere in grado di comprovarne il corretto adempimento.

Ai titolari, altresì, viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri indicati dal regolamento.

Come specifica chiaramente l'articolo 25 del Regolamento 2016/679/UE, uno di quei criteri è sicuramente rappresentato dall'espressione anglofona *data protection by default and by design*, ossia dalla necessità di configurare il trattamento prevedendo dall'inizio, ovvero fin dalla fase di progettazione, le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Spetta dunque al titolare mettere in atto una serie di misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.

Tra le nuove attività previste dal Regolamento 2016/679/UE, riguardo agli obblighi dei titolari, saranno fondamentali quelle relative alla valutazione del rischio inerente il trattamento. Quest'ultimo è da intendersi come rischio da impatti negativi sulle libertà e sui diritti degli interessati. Tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per diminuirne l'impatto.

Una lettura organica e sistematica del Regolamento europeo consente di affermare che, data l'importanza della normativa e di ciò che essa mira a proteggere, la migliore risposta in termini di cambiamento organizzativo sia quella di realizzare un complessivo "Modello organizzativo e di gestione" per la protezione dei dati personali, considerando come tale un complesso di attività organizzativa, di ruoli, di azioni organizzative, di sistemi mirato al fine

dell'applicazione "ordinata" e completa, nell'azione amministrativa dell'Ente, della normativa sui trattamenti di dati personali. Tale logica di costruzione di un Modello *ad hoc* è, peraltro, simile a quella risultante, in materia di prevenzione della corruzione.

L'adeguamento al Regolamento 2016/679/UE impone al titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, l'approvando Modello organizzativo individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche, logiche, logistiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Al fine di garantire la migliore e più puntuale attuazione del principio di *accountability*, il presente modello organizzativo contiene disposizioni regolamentari minime la cui concreta attuazione è demandata all'organizzazione del personale operante all'interno del Comune di Tresignana, nelle sue articolazioni gerarchiche.

È ammesso (e anzi incoraggiato) l'utilizzo di modulistica differente rispetto a quella allegata al presente modello a condizione che essa ne rispetti i criteri e le regole generali.

Il presente modello organizzativo sarà sottoposto a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza triennale.

PARTE I - NORME E PRINCIPI GENERALI

I principi generali

Il Comune di Tresignana assicura che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

In attuazione del suddetto principio il Comune assicura che, nello svolgimento dei compiti e funzioni istituzionali, i dati personali siano trattati nel rispetto della legislazione vigente oltre che dei principi fissati dall'articolo 5 del Regolamento 2016/679/UE, che qui sono richiamati:

a) «**liceità, correttezza e trasparenza**»: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) «**limitazione delle finalità**»: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, del Regolamento 2016/679/UE, considerato incompatibile con le finalità del trattamento. Il WP29 scoraggia i titolari dall'utilizzare, nella propria documentazione in materia di dati personali, espressioni del tipo "i dati personali saranno conservati per il periodo di tempo necessario ai fini delle finalità del trattamento". Se necessario, dovranno essere stabiliti periodi di conservazione *ad hoc* per le varie categorie di dati e/o le varie finalità del trattamento, compresi, ove applicabile, i periodi di archiviazione;

c) «**minimizzazione dei dati**»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «**necessità**»: è ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità;

e) «**esattezza**»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

f) «**limitazione della conservazione**»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, del Regolamento 2016/679/UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato;

g) «**integrità e riservatezza**»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

h) «**responsabilizzazione**»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo.

I dati personali

Il Regolamento 2016/679/UE, nel delineare il suo campo di applicazione, definisce il dato personale come qualsiasi informazione riguardante una persona fisica, identificata o identificabile (definita interessato). Si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente con particolar riferimento a un identificativo, come nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali il Comune, titolare del trattamento, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

1) dati personali, come definiti all'articolo 4, paragrafo 1 del Regolamento 2016/679/UE;

2) categorie particolari di dati personali, come definiti dall'articolo 9, paragrafo 1 del Regolamento 2016/679/UE. L'articolo 9 fornisce un elenco esaustivo e non esemplificativo di tale tipologia di dati personali. Essi sono i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, i dati genetici, i dati biometrici, intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

3) dati personali relativi a condanne penali e reati o a connesse misure di sicurezza, di cui all'articolo 10 del Regolamento 2016/679/UE.

Il trattamento dei dati personali

Usando una definizione molto ampia, il regolamento 2016/679/UE definisce il trattamento dei dati personali 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».

Ne deriva, quindi, che si possa parlare di trattamento ogniqualvolta venga posta in essere anche una soltanto delle suesposte operazioni, senza dover necessariamente parlare di un complesso. L'elenco delle operazioni indicate non è tassativo, ma meramente esemplificativo, sebbene ne comprenda la maggior parte. Per tale motivo, esso si estenderà anche a quelle non espressamente previste.

L'attività di trattamento dei dati personali può avvenire sia con mezzi informatici che con mezzi cartacei.

Il Comune tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali, quali identificate da disposizioni di legge, statutarie e regolamentari, e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo.

Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati e autorizzati.

Non è consentito il trattamento da parte di persone non puntualmente autorizzate e istruite in tal senso.

Al fine di garantire la correttezza delle operazioni di trattamento il Comune provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei procedimenti e processi svolti, finalizzata alla compilazione e aggiornamento del registro delle attività di

trattamento di cui all'articolo 30 del Regolamento 2016/679/UE.

Sensibilizzazione e formazione

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Comune sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, questo Comune riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale nonché quella diretta a tutti coloro che hanno rapporti con lo stesso.

Il Comune organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Comune.

La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa e individuale.

PARTE II - PROFILO ORGANIZZATIVO

PROFILO STRUTTURALE

La prima risposta è l'individuazione di una struttura organizzativa per la protezione dei dati personali, che, ovviamente, si sovrapponga, in gran parte, all'attuale struttura amministrativa dell'ente, integrandosi con essa. La creazione di tale struttura, comporta tre azioni principali:

- il disegno di struttura (organigramma) per la tutela del trattamento dei dati personali (Allegato 1);
- la definizione dei ruoli;
- l'individuazione dei soggetti "designati" dal titolare a trattare i dati personali.

Conseguente, alla costruzione, sarà quindi necessario adeguare le competenze mediante la formazione e informazione dei soggetti, abilitando concretamente i soggetti stessi.

Il titolare del trattamento

L'articolo 4, paragrafo 1, n. 7, del Regolamento 2016/679/UE, precisa che il titolare del trattamento (interpretando la norma rispetto all'ente locale) è l'autorità pubblica che, singolarmente o insieme ad altri «*determina le finalità e i mezzi del trattamento di dati personali*».

Il concetto di titolare del trattamento serve a determinare in primissimo luogo chi

risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il Regolamento 2016/679/UE assegna al titolare del trattamento possono così essere riassunte:
a) determinare le finalità ed i mezzi del trattamento dei dati personali. In considerazione del carattere pubblico che contraddistingue questa pubblica amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (articolo 4, paragrafo 1, n. 7);
b) mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento 2016/679/UE (c.d. *accountability*) (articolo 24);
c) garantire che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non li tratti se non è adeguatamente istruito in tal senso (articoli 29 e 32);
d) individuare i responsabili del trattamento, controllarne e garantirne l'operato (articolo 28);
e) agevolare l'esercizio dei diritti dell'interessato (articolo 12) e fornire agli interessati le informazioni previste dal Regolamento 2016/679/UE (articoli 13 e 14);
f) designare il Responsabile della protezione dei dati (articolo 37) ponendolo in grado di svolgere adeguatamente l'attività (articolo 38);
g) istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (articolo 30);
h) effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (articolo 35);
i) comunicare all'autorità di controllo (articolo 33) e all'interessato (articolo 34) eventuali violazioni dei dati personali;
j) ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (articolo 58);
k) rispondere per il danno cagionato dal trattamento che violi il Regolamento 2016/679/UE (articolo 82);
l) rispondere delle violazioni amministrative ai sensi del Regolamento 2016/679/UE (articolo 83).

Organizzazione interna

Alla luce del testo normativo e delle interpretazioni correnti, in particolare il parere n. 1/2010 del WP29 (WP169) e il provvedimento 09-12-1997 dell'Autorità garante per la protezione dei dati personali, intitolato "Precisazioni sulla figura del titolare", si ritiene che titolare sia l'ente locale nel suo complesso, in quanto la legislazione nazionale gli ha affidato il compito di raccogliere e trattare certi dati personali. Esso manifesta la propria volontà attraverso coloro a cui è attribuito il potere di decidere per l'ente, nell'ambito delle suddivisioni di ruolo nascenti dal diritto amministrativo.

Le competenze e le responsabilità quali delineate dal Regolamento 2016/679/UE e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi di governo del Comune in relazione alle funzioni agli stessi assegnati dal decreto legislativo 18 agosto 2000, n. 267, e dallo Statuto comunale. Tale ripartizione è così intesa:
A. al Consiglio comunale sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;
B. all'organo esecutivo (Giunta comunale) sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del Consiglio, con particolare riferimento agli atti

e attività a contenuto organizzativo e di indirizzo;
C. all'organo di vertice (Sindaco) competono le nomine e le designazioni rilevanti in materia di protezione dei dati personali;
D. Responsabili di posizione di elevata qualificazione, secondo l'ambito di competenza, spettano i seguenti compiti (con elencazione meramente esemplificativa):

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;

b) disporre, in conseguenza alla verifica di cui alla lettera a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;

c) adottare soluzioni di *privacy by design* e *by default*;

d) contribuire al costante aggiornamento del registro delle attività di trattamento;

e) garantire la corretta informazione e l'esercizio dei diritti degli interessati;

f) individuare i soggetti autorizzati a compiere operazioni di trattamento, nel rispetto di quanto previsto dall'articolo 29 del Regolamento 2016/679/UE, fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;

g) disporre l'adozione dei provvedimenti imposti dal Garante;

h) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

i) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;

j) garantire al Responsabile della protezione dei dati personali e al personale (eventualmente) designato Amministratore di sistema i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

k) la preventiva valutazione d'impatto ai sensi dell'articolo 35 del Regolamento 2016/679/UE, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

l) consultare il Garante, in aderenza all'articolo 36 del Regolamento 2016/679/UE, e nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;

m) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;

n) individuare i responsabili del trattamento, ai sensi dell'articolo 28 del Regolamento 2016/679/UE, fornendo le necessarie indicazioni.

Il contitolare del trattamento

La contitolarità del trattamento si verifica nel caso in cui vi sia una determinazione congiunta delle finalità e dei mezzi del trattamento da parte di più soggetti.

In base alla previsione contenuta nell'articolo 26 del Regolamento 2016/679/UE:
«*1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal*

diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati».

Le Linee guida n. 7/2020 dell'*European Data Protection Board* (EDPB) hanno chiarito che il criterio generale per valutare la sussistenza di una contitolarità del trattamento è costituito dalla partecipazione congiunta di due o più soggetti alla determinazione delle finalità e mezzi dello stesso. Tale partecipazione congiunta alla determinazione di finalità e mezzi del trattamento può assumere la forma di una decisione comune o decisioni convergenti dei diversi soggetti coinvolti, che si integrano a vicenda e sono necessarie affinché il trattamento in questione abbia luogo. In sostanza si ha una decisione congiunta rispetto a finalità e mezzi del trattamento quando lo stesso non sarebbe possibile senza la partecipazione delle diverse parti coinvolte, nel senso che i trattamenti di ciascuna parte sono tra loro "indissolubilmente legati".

In coerenza con la propria missione e i propri valori, i contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o a operare con i medesimi ("interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del Regolamento 2016/679/UE.

Spetta ai Responsabili di posizione di elevata qualificazione identificare gli eventuali contitolari di riferimento della struttura organizzativa di competenza, avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai contitolari l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari risultano autorizzate al trattamento dei dati e a compiere le relative operazioni.

La sottoscrizione degli accordi interni per il trattamento dei dati personali verrà effettuata dal Sindaco, in qualità di rappresentante legale *pro tempore* del Comune di Tresignana.

Ciascuno dei contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dall'accordo. Il nominativo e i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

I contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun contitolare.

I contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali. È tuttavia ammessa una diversa ripartizione interna del profilo di responsabilità, da valutarsi caso per caso.

Il responsabile del trattamento

L'articolo 4, paragrafo 1, n. 8, del Regolamento 2016/679/UE, definisce il responsabile del trattamento come «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*». In altre parole è colui che persegue le finalità di trattamento definite dal titolare.

L'esistenza di un responsabile del trattamento dipende da una decisione presa dal titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità - o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.

A norma dell'articolo 28, paragrafo 1, del Regolamento 2016/679/UE: «*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in*

atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato».

Per poter agire come responsabile del trattamento occorrono quindi due requisiti: essere un soggetto distinto dal titolare ed elaborare i dati personali per conto di quest'ultimo.

La liceità dell'attività di trattamento dei dati da parte del responsabile è determinata dal mandato ricevuto dal titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il responsabile diventa (con)titolare.

Si deve tuttavia prendere atto del fatto che esistano situazioni in cui la relazione tra il titolare e un altro soggetto, pubblico o privato, possa generare dei dubbi in merito alla corretta qualificazione del ruolo soggettivo rivestito (titolare o responsabile). Con riferimento a tali fattispecie, questo ente adotta il criterio della valutazione delle circostanze di fatto, suggerito dal Gruppo di Lavoro *ex* articolo 29 nel Parere 1-2010.

L'articolo 28, paragrafo 3, del Regolamento 2016/679/UE prevede che: «*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*».

Il paragrafo 9 del medesimo articolo, da ultimo, prevede che: «*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*».

Spetta a ciascun Responsabile di posizione di elevata qualificazione identificare i responsabili del trattamento, nonché redigere e sottoscrivere i negozi giuridici per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione e acquisire dai responsabili del trattamento e dagli eventuali sub-responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi, risultano autorizzate al trattamento dei dati e a compiere le relative operazioni.

Per un modello di atto di nomina a responsabile del trattamento si veda l'Allegato 2.

Il Responsabile di posizione di elevata qualificazione in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni. L'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.

La periodicità delle predette verifiche, previste nel negozio giuridico di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse sono registrate in apposito verbale, sottoscritto con firma digitale o, se sottoscritto con firma olografa, in duplice originale, dal responsabile del trattamento e dal Responsabile di posizione di elevata qualificazione che svolge ciascuna verifica.

Il responsabile della protezione dei dati personali - *Data protection officer*

Nel rispetto di quanto previsto dagli articoli 37 e ss. del Regolamento 2016/679/UE, il Comune si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD o DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.

Il responsabile della protezione è designato con decreto del Sindaco non oltre sei mesi dalla data della sua proclamazione a seguito dell'individuazione, effettuata con le modalità dell'evidenza pubblica, da parte dell'Unione dei Comuni Terre e Fiumi. Sino alla designazione del nuovo responsabile della protezione dei dati si intende prorogata di diritto la designazione

del responsabile della protezione dei dati in carica al momento della predetta proclamazione. Tale proroga è valida anche a seguito della nomina di un commissario che sostituisca tutti gli organi di governo dell'ente, salvo che lo stesso commissario non ritenga necessario designare un nuovo responsabile della protezione dei dati ovvero sostituire il responsabile in carica all'atto della sua nomina.

I dati identificativi e di contatto del responsabile della protezione dei dati sono pubblicati nel sito informatico istituzionale dell'ente, nella sezione 'Amministrazione trasparente – Altri contenuti – Privacy', comunicati all'Autorità di controllo, comunicati ai componenti degli organi di governo, a tutti i Responsabili di settore e ai dipendenti comunali, ai componenti degli organi di controllo interni. Essi sono altresì inclusi in tutte le informative rese agli interessati ai sensi degli articoli 13 e 14 del Regolamento 2016/679/UE.

I responsabili di posizione di elevata qualificazione (p.e.q.) - designati al trattamento

Il Regolamento 2016/679/UE non prevede espressamente la figura degli "autorizzati/designati/incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'articolo 29, rubricato "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", il quale stabilisce che: «*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*».

Il decreto legislativo 30 giugno 2003, n. 196, all'articolo 2-quaterdecies prevede che:
«*1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.*
2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta».

Conformemente alle disposizioni del Regolamento 2016/679/UE e del decreto legislativo 30 giugno 2003, n. 196, nel suo testo vigente, il titolare e il responsabile del trattamento possono quindi designare, sotto la propria responsabilità e all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati.

Il Regolamento 2016/679/UE e la normativa nazionale di adeguamento consentono dunque di mantenere le funzioni e i compiti assegnati a figure interne al Comune che, ai sensi del decreto legislativo 30 giugno 2003, n. 196, nel testo previgente all'adeguamento al Regolamento europeo, potevano essere definiti come "incaricati".

Il personale operante (a qualunque titolo e a qualunque livello) all'interno del Comune è conseguentemente autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al presente modello organizzativo.

Spetta al Sindaco identificare e designare i Responsabili di posizione di elevata qualificazione, cui assegnare lo svolgimento di specifici compiti e funzioni.
Per un modello di atto di nomina a designato al trattamento, si veda l'Allegato 3.

Il soggetto autorizzato al trattamento

Il Regolamento 2016/679/UE e la normativa nazionale di adeguamento consentono di mantenere le funzioni e i compiti assegnati a figure interne al Comune che, ai sensi del decreto legislativo 30 giugno 2003, n. 196, nel testo previgente all'adeguamento al Regolamento europeo, potevano essere definiti come "incaricati".

Il personale operante (a qualunque titolo e a qualunque livello) all'interno del Comune è conseguentemente autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al presente modello organizzativo.

Spetta ai Responsabili di posizione di elevata qualificazione identificare e designare, per iscritto e in numero sufficiente a garantire la corretta gestione del trattamento dei dati, le persone fisiche della struttura organizzativa dell'ente che operano sotto la diretta autorità del titolare e attribuire loro specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni e controllando costantemente che le operazioni di trattamento siano effettuate in attuazione dei principi di cui all'articolo 5 del Regolamento 2016/679/UE.

Per un modello di atto di nomina ad autorizzato al trattamento, si veda l'Allegato 4.

Il referente del responsabile per la protezione dei dati personali

Ai sensi dell'articolo 38 del Regolamento 2016/679/UE, il titolare ha l'obbligo di assicurarsi che «*il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali».* Il titolare inoltre sostiene «*il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*».

L'ente potrà, pertanto, individuare uno o più dipendenti interni all'ente cui assegnare il compito di "referente" al fine di supportare l'attività del DPO, nelle seguenti attività:

a) informazione e consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento 2016/679/UE. Tale attività comporta il supporto nella redazione di pareri, note, circolari, *policy*, *newsletter* con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori *best practice* in materia di analisi e valutazione dei rischi;

b) sorveglianza dell'osservanza del Regolamento 2016/679/UE, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare 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;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento 2016/679/UE. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei *software* e della relativa documentazione tecnica;

d) cooperare con l'Autorità di controllo e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva prevista dall'articolo 36 del Regolamento 2016/679/UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.

Il referente è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri

compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al DPO ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.

Ove i compiti assegnati al referente vengano svolti in modo collettivo da parte di un *team*, dovrà essere designato un soggetto coordinatore.

Amministratore del sistema informatico

Al fine di ottemperare a quanto disposto dall'Autorità garante per la protezione dei dati personali con il provvedimento del 27-11-2008 (G.U. n. 300 del 24-12-2008), avente a oggetto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e successive modifiche, il titolare si avvale di un amministratore del sistema informatico. Ciò a garanzia che il sistema informatico di questo ente sia strutturato e gestito in modo da consentire l'attuazione delle misure tecniche e organizzative adeguate alla necessaria protezione dei dati personali trattati attraverso lo stesso.

L'amministratore del sistema deve essere in possesso di titolo di studio specifico in informatica, almeno di scuola media di secondo grado o laurea triennale, e di comprovate conoscenze specialistiche tecniche e giuridiche in materia di sicurezza degli strumenti e dei programmi informatici per la protezione dei dati personali nonché della capacità di assolvere i compiti di competenza.

Amministratore del sistema informatico può essere designato un dipendente comunale a tempo indeterminato, inquadrato almeno nella categoria degli istruttori amministrativi, oppure, nel caso di mancanza di un dipendente, un soggetto esterno, persona fisica o giuridica.

Nell'atto o nel contratto di servizio, con cui è designato l'amministratore di sistema, tenuto conto di ciò che comporta sia sul piano delle procedure amministrative sia dell'organizzazione sia dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali, devono essere riportati, altresì, tutti gli adempimenti imposti dalle fonti di diritto europee e nazionali, dal "Gruppo di Lavoro europeo ex art. 29", dall'Autorità garante per la protezione dei dati personali, dalle disposizioni regolamentari e dalle direttive emanate dal titolare del trattamento e dal responsabile della protezione dei dati.

Inoltre, per conformarsi alla disciplina del Codice dell'amministrazione digitale di cui al decreto legislativo n. 7 marzo 2005, n. 82 e successive modifiche, dovrà essere indicato il rispetto dei seguenti adempimenti:

a) gestire l'*hardware* e i *software* dei server e delle postazioni di lavoro informatizzate;

b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;

c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema;

d) impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per i designati e autorizzati al trattamento dei dati personali e per tutti coloro che sono autorizzati all'accesso ai dati contenuti nelle banche dati informatizzate;

e) verificare costantemente che il Comune abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo senza indugio agli adeguamenti eventualmente necessari.

All'amministratore del sistema informatico è:

a) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema, a meno che questo non sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati;

b) obbligato a dare tempestiva comunicazione al Sindaco e ai responsabili del trattamento interessati nonché al responsabile della protezione dei dati dei problemi di affidabilità sia dell'*hardware* che dei *software* eventualmente rilevati;
c) obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici sia da intrusioni che da eventi accidentali.

Il responsabile della protezione dei dati procederà periodicamente alla verifica delle attività svolte dall'amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

PARTE III – ADEMPIMENTI E PROCEDURE

Registro delle attività di trattamento

Ai sensi dell'articolo 30 del Regolamento 2016/679/UE «*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*». La medesima norma individua il contenuto minimo di tale registro, specificando poi che esso è tenuto in forma scritta, anche in formato elettronico, e dev'essere messo a disposizione dell'autorità di controllo.

La tenuta di siffatto registro si configura pertanto come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal Regolamento 2016/679/UE e non soltanto come strumento operativo di mappatura dei trattamenti effettuati.

Un'altra grande differenza rispetto al decreto legislativo 30 giugno 2003, n. 196, è la modalità di mantenimento di tale documento. Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato.

È intenzione del Comune aggiornare il registro dei trattamenti almeno ogni due anni. Il registro dovrà rispettare il contenuto prescritto dal Regolamento 2016/679/UE e dovrà tener conto delle prescrizioni impartite dal Gruppo di lavoro *ex* articolo 29 (ora Comitato europeo per la protezione dei dati) nonché dall'Autorità garante per la protezione dei dati personali.

L'elaborazione del registro è sottoposta all'approvazione della Giunta comunale con cadenza almeno biennale.

Ai fini della migliore realizzazione del registro dei trattamenti, spetta ai Responsabili di posizione di elevata qualificazione:

- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, in correlazione con i procedimenti/processi svolti dall'Ufficio, al fine di consentire la compilazione del registro;
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli interessati, da sottoporre all'approvazione del titolare;
- contribuire alla tenuta del registro in relazione ai trattamenti della struttura organizzativa di competenza, fornendo le necessarie informazioni e valutazioni.

Qualora il titolare decida di provvedere alla gestione e aggiornamento del registro, senza avvalersi di un soggetto esterno, dovrà designare allo scopo un Responsabile di posizione di elevata qualificazione in modo da garantirne l'effettività. Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamento è

demandata alla figura del DPO. Ai sensi dell'articolo 39 del Regolamento 2016/679/UE, che disciplina infatti le prerogative del Responsabile della protezione dei dati personali, si evince che tra le altre è tenuto a «*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati 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*».

All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunge il principio di *accountability* che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della compliance normativa.

Misure per la sicurezza dei dati personali

Nel rispetto di quanto previsto dall'articolo 32 del Regolamento 2016/679/UE, la Giunta comunale, i Responsabili di posizione di elevata qualificazione e l'Amministratore del sistema informatico provvedono, per quanto di rispettiva competenza, all'adozione e alla dimostrazione di aver adottato le misure tecniche e organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche e organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Violazione dei dati personali

Per violazione dei dati personali (in seguito *data breach*) si intende la violazione di sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal titolare (tale indicazione operativa pertanto si applica a tutti gli archivi/documenti cartacei e a tutti i sistemi, anche informativi sui quali siano conservati i dati personali degli interessati, quali cittadini, dipendenti, fornitori, soggetti terzi, *et cetera*).

La segnalazione di un possibile *data breach* può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali *et cetera*) o dall'interno, da parte delle varie funzioni di settore durante il normale svolgimento dell'attività lavorativa (più frequentemente tali eventi vengono evidenziati da funzioni che svolgono attività di verifica e/o di controllo).

Colui che riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di violazione di dati personali, deve darne immediata notizia al Responsabile di elevata qualificazione competente in relazione al trattamento dei dati personali, il quale conduce l'analisi volta ad individuare il grado di probabilità che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Tale analisi è condotta congiuntamente ad altri Responsabili di posizione di elevata qualificazione in caso di trattamento di dati personali coinvolgente diversi uffici o servizi e deve essere accompagnata dall'acquisizione di ogni documento e informazioni utile allo scopo.

Il Responsabile di Responsabile di posizione di elevata qualificazione competente in ragione del trattamento coinvolto, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede a informare immediatamente il Sindaco e il DPO, direttamente ovvero attraverso la figura del referente, se istituita, nonché alla notifica della violazione all'Autorità di controllo.

La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Qualora la notifica effettuata nelle 72 ore non sia completa è possibile integrarla in una o più fasi successive (ad esempio nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo).

Nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro. Il dipendente, responsabile di un trattamento, eventualmente coinvolto deve:

a) informare il Responsabile di posizione di elevata qualificazione tempestivamente e in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, di essere venuto a conoscenza di una violazione;

b) fornire tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Comune e sugli interessati coinvolti e le misure adottate per mitigare i rischi;

c) fornire assistenza per far fronte alla violazione e alle sue conseguenze soprattutto in capo agli interessati coinvolti.

Il Responsabile p.e.q. si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive all'Ufficio e attuando tutte le azioni correttive approvate e/o richieste dall'Ufficio medesimo.

Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito. Risulta opportuno e di particolare importanza che tutti gli atti di designazione a responsabile del trattamento contengano una espressa previsione circa la necessità di informare il titolare, senza ingiustificato ritardo, in caso di avvenuta conoscenza di una violazione di dati personali, anche solo probabile o possibile.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del Regolamento 2016/679/UE, sono i seguenti:

a) danni fisici, materiali o immateriali alle persone fisiche;

b) perdita del controllo dei dati personali;

c) limitazione dei diritti, discriminazione;

d) furto o usurpazione d'identità;

e) perdite finanziarie, danno economico o sociale;

f) decifratura non autorizzata della pseudonimizzazione;

g) pregiudizio alla reputazione;

h) perdita di riservatezza dei dati personali protetti da segreto professionale (come sanitari o giudiziari).

Nel rispetto dell'articolo 34 del Regolamento 2016/679/UE, ove il Responsabile di p.e.q. ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. Prima di procedere alla comunicazione della violazione ai soggetti interessati, il testo della comunicazione, le modalità di notifica e le evidenze che attestano il reale livello di

pregiudizio, dovranno essere concordate con il DPO. Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche sull'evento *data breach*, il Responsabile di p.e.q. può chiedere all'Autorità di controllo l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

La probabilità e la gravità del rischio, per i diritti e le libertà dell'interessato, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio semplice o un rischio elevato. I rischi per i diritti e le libertà degli interessati possono essere considerati elevati quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica all'Autorità di controllo deve avere il contenuto minimo previsto dall'articolo 33 del Regolamento 2016/679/UE, e anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al predetto articolo.

Ciascun Ufficio deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze a esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.

È comunque opportuno che l'inventario delle violazioni tenga traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione. L'inventario dovrà essere dotato di idonee misure di sicurezza atte a garantire l'integrità e l'immodificabilità dei dati in esso registrati.

Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di controllo al fine di verificare il rispetto delle disposizioni del Regolamento 2016/679/UE.

Valutazioni di impatto sulla protezione dei dati

Nel caso in cui una tipologia 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 Responsabile di p.e.q. competente in relazione al trattamento interessato, prima di effettuarlo, deve attuare una valutazione dell'impatto del trattamento medesimo (DPIA), ai sensi dell'articolo 35 del Regolamento 2016/679/UE, considerando la natura, l'oggetto, il contesto e le finalità del trattamento.

La valutazione dell'impatto (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi. Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo processo di DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità di controllo ai sensi dell'articolo 35, paragrafi 4-6, del Regolamento 2016/679/UE. L'Autorità garante per la protezione dei dati personali ha adottato il provvedimento n. 467 del 11-10-2018 [doc. web. n. 9058979], pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di *privacy by design* e *by default* per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi.

L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità. Il Responsabile di p.e.q. conduce quindi una prima fase di valutazione preliminare, il cui scopo è quello di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento sia conforme al Regolamento 2016/679/UE e, in seconda battuta, comprendere se quel trattamento debba essere sottoposto ad una valutazione DPIA.

L'attività quindi si scompone di 3 sotto fasi:

a. descrizione del trattamento (le categorie di soggetti interessati dal trattamento, le finalità del trattamento, le categorie di dati oggetto del trattamento, le modalità di trattamento, il luogo di conservazione dei dati trattati, *et cetera*) sulla scorta delle risultanze contenute nell'apposito registro;

b. valutazione della conformità (analisi della necessità e della proporzionalità del trattamento rispetto alle finalità; rispetto dei principi applicabili al trattamento di cui al capo II del Regolamento 2016/679/UE; rispetto dei diritti degli interessati di cui al capo III del Regolamento 2016/679/UE);

c. valutazione della obbligatorietà di condurre una DPIA.

Fermo restando quanto indicato dall'articolo 35, paragrafo 3, del Regolamento 2016/679/UE, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica oppure che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'articolo 9 del Regolamento 2016/679/UE;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il titolare del trattamento, come i dipendenti dell'ente, soggetti con patologie

psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Responsabile di p.e.q. competente, in relazione al trattamento interessato, sentito il Responsabile della protezione dei dati e l'Amministratore del sistema informatico (se esistente), ritenga motivatamente che non possa presentare un rischio elevato.

Il Responsabile di p.e.q. competente in relazione al trattamento interessato può, motivatamente, ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

La DPIA non è necessaria nei casi seguenti:
a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'articolo 35, paragrafo 1, del Regolamento 2016/679/UE;
b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
c) se il trattamento è stato sottoposto a verifica da parte dell'Autorità garante per la protezione dei dati personali prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è inoltre necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità di controllo o dal Responsabile della protezione dei dati personali e che proseguano con le stesse modalità oggetto di tale verifica.

Inoltre, occorre tener conto che le autorizzazioni dell'Autorità di controllo basate sulla direttiva 1995/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.

Una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti.

L'attività si scompone in ulteriori 4 sotto fasi:
a. raccolta delle informazioni per l'analisi dei rischi - informazioni presenti all'interno dei trattamenti, procedimenti coinvolti dal trattamento, finalità dei dati raccolti, flussi informativi, autorizzati all'accesso alle informazioni, asset model a sostegno dei trattamenti (applicativi, hardware, reti, *et cetera*) -. Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato);
b. valutazione dei rischi, di norma sviluppata nel classico concetto di valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromette un *asset* (informativo) (alcuni esempi sono: gli impatti derivanti da una violazione dei dati di identificazione o attinenti l'identità personale; perdite finanziarie o al patrimonio; perdite dovute a frodi; turbamento per la diffusione di una notizia riservata; evento lesivo dei diritti umani inviolabili o dell'integrità della persona; conseguenze di tipo discriminatorio);
c. valorizzazione delle contromisure e rischio residuo. L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile;
d. piano di trattamento dei rischi.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento; i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (*hardware*, *software*, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
1) delle finalità specifiche, esplicite e legittime;
2) della liceità del trattamento;
3) dei dati adeguati, pertinenti e limitati a quanto necessario;
4) del periodo limitato di conservazione;
5) delle informazioni fornite agli interessati;
6) del diritto di accesso e portabilità dei dati;
7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
8) dei rapporti con i responsabili del trattamento;
9) delle garanzie per i trasferimenti internazionali di dati;
10) consultazione preventiva dell'Autorità garante per la protezione dei dati personali;
c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure previste per affrontare e attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il Regolamento 2016/679/UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
e) l'acquisizione del parere del Responsabile della protezione dei dati personali. Assume quindi fondamentale importanza l'attività di formalizzazione dei risultati, la quale consiste nel valutare se le misure individuate sono idonee a mitigare i rischi a un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA e i razionali che determinano la scelta se procedere o meno alla consultazione preventiva.

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un documento finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal Regolamento 2016/679/UE. Il documento deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

L'ufficio può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Responsabile di p.e.q. competente in relazione al trattamento interessato garantisce l'effettuazione della DPIA ed è responsabile della stessa, salvo che ne affidi l'esecuzione ad altro soggetto, anche esterno al Comune.

Il Responsabile di p.e.q. competente in relazione al trattamento interessato deve consultarsi con il Responsabile della protezione dei dati personali anche per assumere la decisione di effettuare o meno la DPIA. Tale consultazione e le conseguenti decisioni assunte dal Responsabile di p.e.q. competente in relazione al trattamento interessato devono essere documentate nell'ambito della DPIA.

L'ufficio deve consultare l'Autorità di controllo prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato (tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il Regolamento 2016/679/UE, in particolare qualora l'ufficio non abbia identificato o attenuato sufficientemente il rischio).

L'ufficio consulta l'Autorità di controllo anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale e alla sanità pubblica.

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo. Salvo diversa disposizione dell'Autorità di controllo è bene che la comunicazione di richiesta di consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es.: p.e.c., lettera raccomandata, *et cetera*) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data. L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

Il processo DPIA deve sempre prevedere un monitoraggio dei risultati raggiunti e un conseguente e costante riesame al fine di garantire nel tempo la mitigazione dei rischi e la conformità al Regolamento 2016/679/UE, anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno ed esterno, finalità del trattamento, strumenti utilizzati, organizzazione comunale, presenza di nuove minacce, *et cetera*).

Il Responsabile della protezione dei dati personali monitora lo svolgimento della DPIA. Può inoltre proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Eventuali Responsabili del trattamento collaborano e assistono l'ufficio oltre che il Responsabile della protezione dei dati nella conduzione della DPIA fornendo ogni informazione necessaria.

L'Amministratore del sistema informatico (se designato) fornisce il necessario supporto al Responsabile di p.e.q. competente in relazione al trattamento interessato per lo svolgimento della DPIA. Può inoltre proporre di condurre una DPIA in relazione ad uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento. Dal punto di vista operativo - considerata la complessità di un processo DPIA e relativa fase di analisi dei rischi – l'ufficio deve adottare strumenti applicativi specializzati in grado di gestire tutte le fasi del processo ed in grado di riproporre la sua applicabilità nel tempo.

Un esempio di un *software* applicativo per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di CNIL (Autorità francese per la protezione dei dati). Il *software*, al quale ha aderito anche l'Autorità di controllo italiana, non costituisce un modello al quale fare sempre riferimento (si ricorda che è stato concepito soprattutto per le PMI), ma può offrire un *focus* sugli elementi principali di cui si compone la procedura di DPIA. Può quindi costituire un utile supporto metodologico e di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate. Può servire inoltre per comprendere meglio quali possono essere i requisiti di base di un applicativo DPIA adeguato alla propria realtà procedendo quindi ad una *software selection* più mirata e consapevole.

È pubblicata sul sito istituzionale dell'ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

PARTE IV – DIRITTI DELL'INTERESSATO

Informativa, comunicazione e modalità trasparenti per l'esercizio dei diritti dell'interessato

Il Comune adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del Regolamento 2016/679/UE nonché per gestire le comunicazioni in merito all'esercizio dei diritti riconosciuti dal Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni di cui agli articoli 13 e 14 del Regolamento 2016/679/UE sono fornite mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti ai quali l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture comunali, nelle sale d'attesa ed in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito informatico istituzionale del titolare;
- in apposita avvertenza inserita nei contratti oppure nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Comune;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutte le comunicazioni dirette all'Amministrazione;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, *et cetera*.

Il Comune agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18 del Regolamento 2016/679/UE.

Nei casi di cui all'articolo 11, paragrafo 2, del Regolamento 2016/679/UE il Comune non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che dimostri che di non essere in grado di identificare l'interessato.

Il Comune fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta di esercizio dei diritti riconosciuti dal Regolamento 2016/679/UE, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa.

Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Comune informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Se non ottempera alla richiesta dell'interessato, il Comune informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese sulla base dei diritti riconosciuti dal Regolamento 2016/679/UE sono gratuite.

Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Comune può:
a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta.

Incombe al Comune l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Fatto salvo l'articolo 11 del Regolamento 2016/679/UE, qualora il Comune nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di esercizio dei diritti riconosciuti dal Regolamento 2016/679/UE, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato. Si ricorda comunque che le richieste alla pubblica amministrazione devono rispettare quanto disposto dall'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nonché quanto disposto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82.