



# COMUNE DI PISTOIA

## DECRETO DEL SINDACO

**N° proposta:**

164

**NUMERO D'ORDINE  
Registro Generale**

**158**

del

**21/12/2021**

### **OGGETTO:**

**NOMINA DESIGNATI AL TRATTAMENTO DEI DATI PERSONALI E MISURE  
OPERATIVE AI SENSI DEGLI ARTT. 25 E 29 DEL REGOLAMENTO U.E. 679/2016**

## IL SINDACO

**Premesso** che il Comune di Pistoia, in persona del Sindaco – Legale Rappresentante *pro tempore*, è il Titolare del trattamento dei dati personali compiuto per lo svolgimento delle relative funzioni istituzionali dalle proprie articolazioni organizzative o da parte di terzi per suo conto e che in qualità di Titolare è tenuto a garantire che il trattamento medesimo si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, in applicazione dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione (salve le norme in tema di conservazione di atti amministrativi), integrità e riservatezza;

**Vista** la deliberazione della Giunta Comunale n. 216 del 11/10/2017 con la quale è stata approvata la nuova struttura organizzativa del Comune di Pistoia stabilendone l'entrata in vigore a decorrere dal 01/11/2017 o dalla diversa data stabilita con decreto sindacale di affidamento degli incarichi dirigenziali;

**Richiamata** la deliberazione della Giunta Comunale n. 28 del 20/02/2019, con la quale veniva modificato il funzionigramma dell'Ente, assegnando la competenza relativa alla privacy al Servizio Sviluppo Economico e Promozione Territoriale;

**Visti** i decreti del Sindaco con i quali sono stati attribuiti gli incarichi di dirigenza dei Servizi dell'Ente ove ogni Dirigente è designato quale Responsabile del trattamento dei dati personali ai sensi dell'art. 29 del D. Lgs. 196/2003 ("Codice in materia di protezione dei dati personali");

**Considerato** che ogni Dirigente in relazione al proprio Servizio, nell'ambito di attribuzioni, funzioni e competenze conferite, ha i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;

**Visto** il decreto del Sindaco n. 49 del 29/03/2019, contenente la più specifica designazione dei Dirigenti a Responsabili del trattamento dei dati personali e l'autorizzazione degli stessi alla nomina dei Responsabili esterni ai sensi dell'art. 29 del D. Lgs. 196/2003 ("Codice in materia di protezione dei dati personali");

**Dato atto** che nel corso dell'anno 2020 e 2021 il Comune di Pistoia è stato interessato da importanti cambiamenti organizzativi con l'assunzione di nuovi dirigenti e dipendenti, oltre al cambio di alcuni responsabili titolari di posizione organizzativa, operazioni che hanno comportato una ulteriore ridefinizione della macrostruttura dell'Ente con Deliberazioni della Giunta Comunale n. 285 del 16/12/2020 e n. 15 del 17/02/2021;

**Visto** il Regolamento Europeo n. 679/2016 del 27/04/2016 ("Regolamento Generale sulla protezione dei dati" – GDPR), ed in particolare gli articoli 25 e 29 secondo i quali il Responsabile/Designato del trattamento che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento;

**Ritenuto** di dover procedere ai sensi dell'art. 29 GDPR sopra richiamato a fornire le necessarie misure operative, elaborate dall'Ufficio Privacy con il supporto del DPO, ai Dirigenti ed al Segretario Generale, designati ciascuno per le proprie funzioni di competenza affinché possano mettere in atto misure procedurali ed organizzative volte a garantire uniformemente all'interno dell'Ente il rispetto degli adempimenti e degli obblighi di cui al Regolamento Europeo n. 679/2016. Tali misure operative di carattere generale dovranno essere altresì adattate da ciascun Dirigente, qualora intervenissero variazioni significative nel quadro normativo europeo e nazionale o di carattere tecnologico-informatico;

**Dato atto** che, ai fini degli adempimenti in carico ai Designati al Trattamento, si ritiene opportuno prevedere lo specifico supporto da parte dell'Ufficio Privacy e dei Servizi Informativi ed Informatici oltre che quello del DPO, il quale svolge funzioni di consulenza e vigilanza sull'operato dell'Amministrazione in relazione alla privacy;

### **Richiamati**

- il vigente Regolamento sull'ordinamento degli uffici e dei servizi, e, in particolare, la disciplina relativa al conferimento degli incarichi dirigenziali;
- le vigenti disposizioni contrattuali relative al personale di qualifica dirigenziale del comparto Regioni e Autonomie locali in materia di conferimento di incarichi dirigenziali;
- l'art. 19 del vigente D. Lgs. 165/2001;
- l'art. 50, comma 10, D. Lgs. 267/2000 e l'art. 20 del vigente Statuto Comunale, che stabiliscono le competenze del Sindaco in merito all'attribuzione e alla definizione degli incarichi dirigenziali;

**Sentita** la Giunta Comunale;

**Ritenuto** di dover provvedere in ordine a quanto sopra;

## **D E C R E T A**

- **Di confermare** la nomina a Designati del trattamento dei dati personali, ai sensi dell'art. 29 del Regolamento Europeo n. 679/2016 dei Dirigenti *pro tempore*, ciascuno per le proprie funzioni nell'ambito del Servizio di appartenenza, nonché il Segretario Generale per le funzioni di competenza. I Designati dovranno osservare le misure operative di seguito riportate e relative a:

- 1- *Finalità del trattamento*
- 2 - *Designati del trattamento*
- 3 - *Autorizzati al trattamento*
- 4 - *Responsabile esterno del trattamento*
- 5 - *Informativa privacy*
- 6 - *Registro Unico delle attività di trattamento*
- 7 - *Valutazione di impatto sulla protezione dei dati (DPIA)*
- 8 - *Diritti dell'interessato*
- 9 - *Obblighi di trasparenza*
- 10 - *Data breach*
- 11 - *Sensibilizzazione e formazione del personale*

- **Di precisare** che tali misure operative di carattere generale dovranno essere altresì adattate da ciascun Dirigente, qualora intervenissero variazioni nel quadro normativo europeo e nazionale o di carattere tecnologico-informatico.

\*\*\*

### **1 - Finalità del trattamento**

1. Il trattamento dei dati personali è compiuto dal Designato al trattamento per le seguenti finalità:

- a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
- b) l'adempimento di un obbligo legale al quale è soggetto il Comune;

- c) l'esecuzione di un contratto con soggetti Interessati o per la conclusione dello stesso;
- d) la salvaguardia degli interessi vitali dell'Interessato persona fisica;
- e) specifiche finalità diverse da quelle di cui alle precedenti lettere, purché l'Interessato esprima il consenso al trattamento.

2. Rientrano nelle finalità di cui al comma 1, lett. a), i trattamenti compiuti per:

- l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale o regionale affidate al Comune in base alla legislazione vigente ovvero per altri servizi in base a convenzione;
- la tutela in giudizio del Comune.

## **2 - Designati al trattamento**

1. Designati al trattamento sono Il Segretario Generale ed singoli Dirigenti *pro tempore*, i quali, nell'ambito della propria struttura organizzativa ed in relazione al settore di propria competenza, assicurano il rispetto degli obblighi normativi previsti in capo al Titolare del trattamento.

2. I Designati al trattamento provvedono a:

- a) censire e monitorare costantemente le singole attività di trattamento dei dati personali facenti capo al Servizio di propria competenza, verificando l'adeguatezza delle misure di sicurezza adottate;
- b) fornire prontamente ogni elemento necessario alla regolare tenuta del Registro Unico delle attività di trattamento predisposto dal Comune di Pistoia al fine di consentire il costante aggiornamento dello stesso; a tal fine, in particolare, ogni Dirigente aggiorna semestralmente, entro il 30 giugno ed entro il 31 dicembre di ogni anno, la scheda del Registro relativa al proprio Servizio e la invia all'Ufficio Privacy;
- c) designare con atto scritto i soggetti autorizzati al trattamento dei dati personali, sia appartenenti al proprio Servizio che appartenenti ad altri Servizi dell'Ente, qualora questi ultimi abbiano accesso a banche dati ed in generale a dati personali detenuti e trattati dal proprio Servizio;
- d) vigilare sull'attività dei soggetti Autorizzati al trattamento e garantirne una adeguata formazione nell'ambito delle iniziative predisposte dall'Ente e dal Responsabile della Protezione dei dati (DPO);
- e) specie nel caso di trattamento da effettuarsi attraverso l'uso di tecnologie che possano presentare un elevato rischio per i diritti e le libertà delle persone fisiche, effettuare apposita analisi del rischio, predisponendo, ove necessario, la valutazione di impatto ai sensi dell'art. 35 GDPR (DPIA), considerati la natura, l'oggetto, il contesto e le finalità del trattamento dei dati;
- f) segnalare immediatamente al DPO ed all'Ufficio Privacy del Comune la violazione dei dati personali (c.d. *data breach*) al fine della tempestiva notifica al Garante della Privacy;
- g) garantire l'esercizio dei diritti da parte degli interessati, dando corso alle relative richieste;
- h) predisporre, ove ne ritengano la necessità, le informative privacy relative al proprio Servizio e/o allo specifico settore di competenza, provvedendo alla loro massima diffusione attraverso la pubblicazione sul sito web istituzionale dell'Ente e nella propria

area tematica in particolare, oltre che attraverso l'affissione nei locali adibiti al pubblico, curandone l'aggiornamento;

i) nominare eventuali Responsabili esterni del trattamento dei dati e fornire annualmente l'elenco aggiornato dei Responsabili esterni all'Ufficio Privacy;

l) informare il DPO e l'Ufficio Privacy dei nuovi trattamenti effettuati al fine di ottenere da questi ultimi eventuali informazioni in merito agli specifici adempimenti da porre in essere.

### **3 - Autorizzati al trattamento**

1. I Designati al trattamento nell'ambito della propria articolazione organizzativa procedono a nominare con atto scritto il personale dipendente autorizzato per l'espletamento di tutte le operazioni del trattamento dei dati.

2. L'atto di nomina dovrà specificare i compiti affidati agli Autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

3. Gli Autorizzati al trattamento dei dati personali effettuano tutte le operazioni di trattamento dei dati nell'ambito delle mansioni cui sono adibiti, nel rispetto delle istruzioni e direttive che vengono impartite dal proprio Dirigente, che prevedono specificamente di:

a) accedere ai dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;

b) trattare i dati personali di cui si viene a conoscenza per l'espletamento delle proprie funzioni in modo lecito e corretto, nel rispetto delle norme di legge, dello Statuto e dei Regolamenti che disciplinano le attività del Comune;

c) verificare costantemente i dati, il loro aggiornamento, la loro completezza e pertinenza;

d) custodire con cura atti e documenti contenenti dati personali ricevuti in consegna per adempiere ai compiti assegnati e restituirli al termine delle operazioni affidate;

e) comunicare i dati personali trattati solo previa autorizzazione;

f) osservare scrupolosamente le misure di sicurezza predisposte;

g) osservare, anche in seguito a modifica, trasferimento e/o cessazione del rapporto di lavoro gli obblighi relativi alla riservatezza e alla comunicazione.

### **4 - Responsabile esterno del trattamento**

1. Spetta al Segretario Generale ed ai Dirigenti in qualità di Designati al trattamento la nomina dei Responsabili esterni, con la quale si provvede ad autorizzare tali soggetti al trattamento dei dati dando adeguate istruzioni in ordine all'oggetto dell'incarico, alla durata, alla natura ed alla finalità del trattamento, oltre a prevedere eventuali obblighi a carico degli stessi in modo da garantire che il trattamento avvenga nel rispetto dei principi di cui all'art. 5 GDPR.

2. La nomina del Responsabile del trattamento può essere contenuta nel contratto di affidamento dell'incarico/servizio ovvero in separato atto giuridico debitamente sottoscritto dalle parti contrattuali, allegato al contratto e facente parte integrante dello stesso.

3. I Responsabili del trattamento sono nominati tra soggetti che risultino in possesso, secondo una prudente valutazione, dei requisiti di esperienza, capacità ed affidabilità e

delle garanzie, anche di sicurezza, di cui all'art. 28 GDPR, la cui sussistenza deve essere espressamente dichiarata nella nomina.

4. I Responsabili esterni hanno l'obbligo di:

a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia, solo per i fini indicati dal contratto e con divieto di qualsiasi altra diversa utilizzazione;

b) adottare tutte le misure di sicurezza, tecniche ed organizzative, idonee a prevenire e/o evitare la comunicazione e/o la diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso o di trattamento non autorizzato o non conforme alle finalità dello stesso;

c) nominare i soggetti autorizzati al trattamento, garantendo che gli stessi si impegnino formalmente alla riservatezza, che siano adeguatamente formati in materia di protezione dei dati personali prima che inizino il trattamento e limitando solo a questi ultimi il trattamento dei dati personali;

d) redigere, ai sensi dell'art. 30 GDPR, qualora ne ricorrano i presupposti, il registro delle attività di trattamento;

e) mettere a disposizione del Titolare e dei Designati al trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal GDPR e dalle presenti Disposizioni Tecniche ed Organizzative;

g) informare - tempestivamente il Titolare ed i Designati al trattamento di tutte le questioni riguardanti il trattamento dei dati personali;

h) assistere e collaborare con il Titolare ed i Designati al trattamento in caso di richiesta finalizzata all'esercizio dei diritti da parte dell'Interessato al fine di soddisfare il relativo obbligo da parte del Titolare/Designati al trattamento;

i) assistere e collaborare con il Titolare ed i Designati al trattamento al fine di predisporre la valutazione di impatto sulla protezione dei dati connessa al trattamento effettuato;

l) informare il Titolare ed i Designati al trattamento, immediatamente e senza ritardo, della conoscenza di casi di violazione dei dati personali (c.d. "data breach") per la successiva notifica della violazione al Garante della Privacy, indicando:

- il numero di Interessati coinvolti e se sono identificabili;
- la tipologia di dati personali violati (se ordinari, particolari, giudiziari) o se sono coinvolti minori;
- la valutazione dell'impatto della violazione e della gravità delle conseguenze per gli Interessati;
- la durata della violazione;
- il danno/evento verificatosi nel caso specifico, dando informazioni dettagliate al riguardo, le procedure adottate per contenere la violazione, indicando se sono stati ripristinati i dati e/o arginati i danni dagli informatici, e le misure di sicurezza da adottare/adottate al fine di attenuare i possibili ulteriori effetti negativi ed affinché la violazione non si ripeta;
- tutti i parametri necessari per la valutazione del rischio (soprattutto per violazioni informatiche), specificando se la violazione mette a rischio i diritti e le libertà degli Interessati coinvolti, indicando altresì quale è il livello di rischio dell'evento fra *nessun rischio* - *presenza di rischio* - *rischio elevato*;

m) alla cessazione del rapporto, cancellare i dati trattati per conto del Titolare del trattamento, dopo averne predisposto copia di back-up completa da consegnare a quest'ultimo; una volta verificata l'integrità della copia, il Titolare/Designato al trattamento autorizzerà la definitiva cancellazione tramite pec o altro mezzo equipollente;

5. Il Responsabile esterno del trattamento potrà ricorrere, previa autorizzazione scritta del Designato al trattamento, ad uno o più Sub-Responsabili per l'esecuzione di specifiche attività di trattamento ai sensi dell'art. 28 GDPR. Al Sub-Responsabile sono imposti gli stessi obblighi in materia di protezione dei dati previsti dal GDPR e dalle presenti Disposizioni tecniche ed Organizzative in relazione ai Responsabili del trattamento.

## **5 - Informativa privacy**

1. L'informativa privacy deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile. Deve inoltre avere un linguaggio semplice e chiaro.

2. L'informativa è data, in linea di principio, per iscritto, preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, pur nel rispetto delle caratteristiche di cui sopra.

3. Al fine di rendere più agevole la comprensione delle modalità e delle finalità del trattamento dei dati personali all'interessato, ciascun Servizio, in relazione all'attività svolta, è tenuto ad elaborare informative specifiche relative al proprio Servizio.

## **6 - Registro Unico delle attività di trattamento**

Il Registro Unico deve essere periodicamente aggiornato; a tal fine, ogni Dirigente aggiorna semestralmente, entro il 30 giugno ed entro il 31 dicembre di ogni anno, la scheda del Registro relativa al proprio Servizio e la invia all'Ufficio Privacy, che ne cura la raccolta e aggiornamento all'interno del Registro Unico.

## **7 - Valutazione di impatto sulla protezione dei dati (DPIA)**

1. La valutazione di impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento dei dati, valutarne necessità e proporzionalità, nonché a contribuire ad individuare e gestire i rischi per i diritti e le libertà delle persone fisiche connessi al trattamento, al fine di valutare l'adeguatezza e l'idoneità delle misure di sicurezza adottate per fronteggiarli e proporre eventualmente di ulteriori.

2. Considerati il tipo, la natura, il contesto e le finalità di trattamento, qualora esso possa comportare rischi per i diritti e le libertà delle persone fisiche, i Designati, prima di effettuare il trattamento medesimo, devono attuare una valutazione dell'impatto ai sensi dell'art. 35 GDPR.

3. La valutazione deve contenere:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- b) una valutazione della necessità e della proporzionalità del trattamento in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli Interessati;
- d) le misure di sicurezza ed i meccanismi previsti per affrontare i rischi e garantire la protezione dei dati personali.

4. Qualora insorgano variazioni del rischio rappresentato dalle attività relative al trattamento, occorrerà procedere ad un riesame della valutazione di impatto sulla protezione dei dati.

5. Qualora un determinato servizio sia affidato a terzi, Responsabili esterni del trattamento, questi ultimi saranno tenuti ad assistere i Designati del trattamento nella conduzione della valutazione di impatto sulla protezione dei dati, fornendo ogni informazione necessaria.

6. La valutazione di impatto non è ritenuta necessaria nei seguenti casi:

- quando il trattamento non è atto a comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, GDPR;
- quando 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 precedente valutazione, potendosi in tal caso utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- quando il trattamento è stato sottoposto a verifica (terminata positivamente) da parte del Garante della Privacy prima dell'entrata in vigore del GDPR in condizioni specifiche che non hanno subito modifiche;
- quando un trattamento trova la propria base giuridica nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

7. I Designati del trattamento sono tenuti a consultare il Garante della Privacy prima di procedere al trattamento solo se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato in assenza di misure adottate per attenuare il rischio o nei casi in cui la vigente legislazione, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica, stabilisca l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità.

## **8 - Diritti dell'Interessato**

1. I Designati al trattamento garantiscono l'esercizio da parte degli interessati dei diritti di cui agli artt. 15-22 GDPR (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione, ecc.).

2. Ai fini dell'esercizio di tali diritti, la richiesta può essere fatta pervenire alternativamente a mezzo posta elettronica certificata, posta elettronica ordinaria, raccomandata, consegna all'Ufficio del Protocollo o all'URP, destinata:

- a) al Titolare del trattamento;
- b) ai Designati al trattamento;
- c) al DPO;
- d) se il trattamento è effettuato da soggetti terzi per conto del Comune, al Dirigente che ha provveduto alla nomina del Responsabile esterno del trattamento.

3. L'esercizio dei diritti da parte dell'interessato è gratuito e non soggetto al pagamento di diritti di riproduzione e copia.

4. L'Ufficio competente provvede senza ritardo sulla richiesta e comunque entro 30 giorni dal suo ricevimento.



5. Sono fatte salve le limitazioni di cui agli artt. 2 *undecies* e 2 *duodecies* del D. Lgs. 196/2003 e le altre limitazioni previste dalla legge.

## **9 - Obblighi di trasparenza**

1. La protezione dei dati personali incontra un limite negli obblighi di trasparenza imposti all'Ente ai sensi del D. Lgs. 33/2013 e nel dovere di pubblicazione degli atti sancito da specifiche disposizioni di legge.

2. A tal riguardo, possono essere pubblicati esclusivamente i dati personali per i quali è previsto il relativo obbligo, avendo cura di eliminare i dati eccedenti che non possono essere diffusi in un'ottica di contemperamento tra il principio di minimizzazione dei dati e le esigenze di trasparenza.

3. Conseguentemente, ogni qualvolta l'Ente sia tenuto a pubblicare un atto, dovrà prima accertarsi della presenza di una norma di legge o regolamento avente forza di legge che prescrive la pubblicazione, trarne il senso e la finalità e pubblicare solo i dati personali a ciò necessari, non importa se ordinari o meno.

4. In ogni caso, nella pubblicazione di alcune tipologie di atti (es. graduatorie da cui si desume una disabilità o un reddito particolarmente basso tale da ottenere benefici economici), i dati identificativi degli Interessati devono essere adeguatamente pseudonominizzati, ferma restando la conservazione del documento completo senza *omissis* all'interno dell'Ente.

5. E' fatto espresso ed assoluto divieto di pubblicazione di dati sanitari e sulla vita sessuale, dovendosi oscurare del tutto l'identificativo della persona, il quale non deve emergere in alcun modo dalla documentazione pubblicata.

6. La pubblicazione di dati particolari (*ex sensibili*) e di quelli giudiziari può essere effettuata solo se indispensabili al perseguimento della finalità di rilevante interesse pubblico.

7. La durata della pubblicazione dei dati personali per finalità di trasparenza è quello di 5 anni. In tutti gli altri casi i dati sono pubblicati solo per 15 giorni mediante affissione all'Albo Pretorio.

## **10 - Data breach**

1. Qualunque 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 dall'Ente costituisce un *data breach*.

2. Chiunque all'interno dell'Ente venga a conoscenza di un *data breach* è tenuto a segnalarlo immediatamente, anche per il tramite del proprio Dirigente, all'Ufficio Privacy ed ai Servizi Informativi ed Informatici con segnalazione telefonica e invio e-mail al DPO ([dpo@comune.pistoia.it](mailto:dpo@comune.pistoia.it)), ai fini della tempestiva notifica al Garante per la Privacy. Allo

stesso modo procede il Responsabile esterno del trattamento attraverso il Dirigente che ha proceduto all'affidamento del servizio.

3. Entro 72 ore dalla violazione l'Ufficio Privacy, con il supporto del Dirigente del Servizio che ha verificato la violazione dei dati, dei Servizi Informativi ed Informatici e del DPO, provvede alla notifica al Garante per la Privacy, fatta eccezione per i casi in cui il rischio per la tutela dei diritti e delle libertà delle persone fisiche appaia improbabile. La notifica effettuata oltre le 72 ore deve essere specificamente motivata.

4. La notifica deve contenere tutti gli elementi di cui al par. 3 dell'art. 33 del GDPR. A tal fine, ogni Dirigente è tenuto a documentare in modo puntuale le violazioni di dati subite, anche qualora alle stesse non segua notifica al Garante per la Privacy.

5. Nello specifico, in caso di violazione di dati, si dovrà indicare:

- il numero di Interessati coinvolti e se sono identificabili;
- la tipologia di dati personali violati (se ordinari, particolari, giudiziari) o se sono coinvolti minori;
- la valutazione dell'impatto della violazione e della gravità delle conseguenze per gli interessati;
- se sono stati ripristinati i dati e/o arginati i danni dagli informatici;
- la durata della violazione;
- tutti i parametri necessari per la valutazione del rischio (soprattutto per violazioni informatiche);
- dettagliare il danno/evento, le procedure adottate per contenere la violazione e le misure di sicurezza da adottare/adottate al fine di attenuare i possibili effetti negativi e affinché la violazione non si ripeta;
- se la violazione mette a rischio i diritti e le libertà degli interessati coinvolti dalla violazione, indicando altresì quale è il livello di rischio dell'evento fra nessun rischio - presenza di rischio - rischio elevato.

6. Le violazioni dei dati personali, anche non notificate al Garante per la Privacy, saranno annotate nel Registro Accountability tenuto dall'Ufficio Privacy, dove dovranno essere indicate le circostanze relative alle violazioni, le conseguenze e i provvedimenti adottati o che intendano adottare il Titolare e/o i Designati al trattamento per porvi rimedio.

## **11 - Sensibilizzazione e formazione del personale**

1. Ai fini della corretta e puntuale applicazione della disciplina relativa alla protezione dei dati personali, il Designato al trattamento 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.

2. A tale riguardo, uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del Comune e l'attività informativa diretta a tutti coloro che hanno rapporti con il Titolare.

3. Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione e trasparenza, 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.

4. Il Segretario Generale ed i Dirigenti garantiscono la più ampia partecipazione agli eventi formativi di cui sopra.

\*\*\*

**- Di stabilire** che copia del presente decreto sia trasmesso a:

Dott. Raffaele Pancari, Segretario Generale;

Dirigenti Comunali;

Dott. Giorgio Zuccherini, Capo Gabinetto;

Responsabile dell'Ufficio del Consiglio Comunale per l'opportuna conoscenza da parte dei Consiglieri Comunali;

Componenti della Giunta Comunale;  
DPO, Avv. Benedetta De Luca.

Il Sindaco  
(TOMASI ALESSANDRO)