COMUNE DI NEONELI

Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali in conformità alla disciplina di cui al Regolamento UE 2016/679

Approvato con deliberazione del Consiglio Comunale n. 37 del 30.11.2022

SOMMARIO

INTRODUZIONE

Il 27.04.2016 è stato approvato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con abrogazione della direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).
Il predetto regolamento UE, obbligatorio in tutti i suoi elementi e direttamente applicabile a ciascuno degli Stati membri a decorrere dal 25 maggio 2018, si fonda sul principio in forza del quale la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale, come previsto dall'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e dall'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione Europea ("TFUE") che stabiliscono che "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano".
Per rafforzare la richiamata protezione, il Regolamento UE introduce numerose e rilevanti novità, che si fondano sul presupposto che il trattamento dei dati personali sia al servizio della persona, dei sui diritti e delle sue libertà, con particolare riferimento al rispetto della vita privata e familiare, del domicilio, delle comunicazioni, della libertà di pensiero, di coscienza, di religione, della libertà di espressione, di informazione, d'impresa e nel rispetto della diversità culturale, religiosa e linguistica.
La principale novità introdotta dal Regolamento UE riguarda il nuovo approccio al rischio basato sul concetto di accountability, ovvero sul c.d. "principio di responsabilizzazione".
Secondo il Regolamento UE, è il Titolare del trattamento dei dati personali a dover valutare le misure tecniche ed organizzative da adottare sulla base della natura dei dati, dell'oggetto, delle finalità del trattamento.
La sicurezza diventa un concetto dinamico da mettere in costante relazione con le conoscenze acquisite in base al progresso tecnico, alla natura dei dati personali oggetto di trattamento ed alle specifiche caratteristiche delle operazioni di trattamento compiute.
L'individuazione di idonee misure di sicurezza da adottare spetta al Titolare, in esito alla valutazione operata sulla natura dei dati, sul contesto, suoi rischi, sui danni potenziali, sui costi e sullo stato dell'arte.
Come ha evidenziato il Garante per la protezione dei dati personali nella guida all'applicazione del Regolamento UE, la nuova disciplina europea pone con forza l'accento sulla "responsabilizzazione" di Titolari e Responsabili, ossia sull'adozione di comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.
Tra i criteri che i Titolari ed i Responsabili sono tenuti ad utilizzare nella gestione degli obblighi vi sono, in primo luogo, il criterio del "data protection by default and by design", ossia la necessità di configurare fin dalla progettazione ed in modo predefinito la tutela dei dati personali, prevedendo fin dall'inizio l'adozione di misure idonee a garantire un livello di sicurezza adeguato al rischio e a tutelare i diritti degli interessati.
È posto in capo al Titolare ed al Responsabile del trattamento l'obbligo di valutare i rischi inerenti al trattamento, tenendo conto del contesto complessivo nel quale il trattamento si colloca e dei rischi per i diritti e per le libertà degli interessati.
Il criterio del rischio inerente al trattamento deve intendersi come rischio di impatti negativi sulle libertà e sui diritti degli interessati; impatti che devono essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative di sicurezza che il Titolare ed il Responsabile ritengono di dover adottare per mitigare tali rischi.
Ne consegue che l'intervento dell'Autorità di controllo, nel nuovo impianto gestionale, è destinato a svolgersi principalmente "ex post", ossia a collocarsi, sul piano cronologico, in un momento successivo rispetto alle scelte ed alle determinazioni assunte autonomamente dal Titolare e dal Responsabile; ciò spiega l'abolizione, a partire dal 25.05.2018, di alcuni istituti previsti dalla

direttiva del 1995 e dal D.Lgs. 196/2003, come la notifica preventiva dei trattamenti all'Autorità di controllo e la verifica preliminare, sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del Titolare/Responsabile e di effettuazione di valutazioni di impatto in piena autonomia.
Dall'esame complessivo del nuovo quadro normativo di riferimento emerge come sia imprescindibile un cambiamento di mentalità, che porti alla piena tutela del diritto alla riservatezza, da intendersi non più come mero oneroso rispetto di formali adempimenti burocratici ma come garanzia per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza di tipo sostanziale che riguardi la persona in tutte le sue manifestazioni.
Il diritto alla riservatezza è un diritto inviolabile che non si limita alla protezione dei dati, ma implica il pieno rispetto dei diritti, delle libertà fondamentali e della dignità della persona.
Per questi motivi la cultura del diritto alla riservatezza necessita di crescere e rafforzarsi, principalmente all'interno della Pubblica Amministrazione, in quanto solo attraverso una profonda conoscenza dei principi fondamentali che stanno alla base della vigente normativa si potrà dare corso in modo responsabile ai nuovi obblighi previsti dal legislatore comunitario con la consapevolezza di non dover affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con i cittadini.

CAPO I - DISPOSIZIONI GENERALI

Art. 1 – Oggetto

1. Il presente regolamento ha per oggetto le misure procedimentali e le regole di dettaglio da applicare nel Comune ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo "General Data Protection Regulation" del 27.04.2016 n. 679 (di seguito "RGPD"), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati.

Art. 2 - Quadro normativo di riferimento

1. Il presente regolamento tiene conto dei seguenti documenti:
- RGPD UE 679/2016 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;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Codice in materia di dati personali (D.Lgs. n.196/2003), riformato dal D.Lgs. n. 101/2018;
- Linee guida, Provvedimenti e Raccomandazioni del Garante per la protezione dei dati personali;
- Linee guida sui responsabili della protezione dei dati (DPO) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;

- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Linee Guida 07/2020 adottate in data 02 settembre 2020 dal Comitato Europeo per la protezione dei dati le sui concetti *di* "controller" e "processor", equivalenti rispettivamente al Titolare del trattamento ed al Responsabile del trattamento dei dati;
- L. 241/9090 Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- D.Lgs. 33/2013 Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.

Art. 3 – Definizioni

1. Ai sensi dell'art. 4 RGPD, il presente regolamento utilizza le seguenti definizioni:
«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
«Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
«Autorizzato al trattamento»: la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del Titolare o del Titolare di PO/Dirigente designato allo svolgimento di specifici compiti e funzioni connessi al trattamento;
«Titolare di PO/Dirigente Designato allo svolgimento di specifici compiti e funzioni connessi al trattamento»: la persona fisica espressamente designata che, sotto la responsabilità del Titolare e

nell'ambito della propria struttura organizzativa, svolge specifici compiti e funzioni connessi al trattamento dei dati personali;
«Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
«Interessato»: la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
«Destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
«Terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile;
«Consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
«Violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
«Dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
«Dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
«Dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del RGPD;
«Autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto
- il Titolare del trattamento o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
- oppure un reclamo è stato proposto a tale autorità di controllo.

2. Ai sensi dell'art. 2-ter, comma 4, D.Lgs. 196/2003 si intende per:
«comunicazione»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
«diffusione»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 4 - Liceità del trattamento

1. Sono integralmente recepite nell'ordinamento interno del Comune, quale titolare del trattamento dei dati, le disposizioni del RGPD in ordine alla liceità del trattamento; conseguentemente, il trattamento è lecito solo se e nella misura in cui ricorra almeno una delle seguenti condizioni:
a) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune quale titolare del trattamento;
b) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
c) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
d) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Comune quale titolare del trattamento;
e) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.
2. Se il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non è basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il dipendente autorizzato al trattamento dei dati tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Comune quale titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo RGPD;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 5 - Trattamento di categorie particolari di dati personali

1. In attuazione dell'art. 9, paragrafo 1, RGPD, rientrano nella nozione di "categorie particolari di dati personali", i dati idonei a rivelare: 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.
2. È vietato trattare i dati di cui al precedente comma, a meno che non si verifichi uno dei seguenti casi:
a) il trattamento è necessario per motivi di interesse pubblico rilevante previsti dal diritto dell'Unione o nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
Ai sensi dell'art. 2-sexies, comma 2, D.Lgs. 196/2003, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati dal Comune nelle seguenti materie:

- accesso a documenti amministrativi e accesso civico;
- tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
- cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;

- elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
- esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
- svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
- attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;
- attività di controllo e ispettive;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- obiezione di coscienza;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (SISTAN);
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

b) L’interessato ha prestato il proprio consenso esplicito al trattamento di tali categorie particolari di dati personali per una o più finalità specifiche.

c) Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell’interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell’Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell’interessato.

d) Il trattamento riguarda dati personali resi manifestamente pubblici dall’interessato.

e) Il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

f) Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro e per la valutazione della capacità lavorativa del dipendente.

g) Il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 6 - Trattamento di dati personali relativi a condanne penali e reati

1. In attuazione dell'art. 10 RGPD, rientrano nella nozione di "dati personali relativi a condanne penali e reati", i dati personali relativi alle condanne penali, ai reati o alle connesse misure di sicurezza.
2. Fatto salvo quanto previsto dal d.lgs. n. 51/2018, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza che non avviene sotto il controllo dell'autorità pubblica, è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.
3. Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:
a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi;
b) la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
c) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
e) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto.

CAPO II - SOGGETTI DEL TRATTAMENTO

Art. 7 – Il Comune quale titolare del trattamento

1. In attuazione dell'art. 4, paragrafo 1, n. 7, RGPD, il titolare del trattamento dei dati del Comune è l'Ente nel suo complesso. Il legale rappresentante del Comune è il Sindaco.
2. Il Comune nel suo complesso è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; aggiornamento e limitazione della conservazione; integrità e riservatezza.
3. I dipendenti autorizzati al trattamento dei dati mettono in atto misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento di dati personali sia effettuato in modo conforme al RGPD, con particolare riferimento all'adozione delle misure di sicurezza di cui all'art. 32 RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli artt. 15-22 RGPD.
4. Gli interventi necessari all'attuazione delle misure sono stabiliti in apposite direttive della Giunta Comunale, previa analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

5. I dipendenti autorizzati al trattamento dei dati adottano misure appropriate per fornire all'interessato le informazioni indicate dall'art. 13 RGPD qualora i dati personali siano raccolti presso lo stesso interessato e le informazioni indicate dall'art. 14 RGPD qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
6. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Responsabile di Servizio dispone l'effettuazione di una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito "DPIA") ai sensi dell'art. 35 RGDP, in ragione della natura, dell'oggetto, del contesto e delle finalità del medesimo trattamento, sulla base dell'elenco delle tipologie di trattamento da sottoporre a valutazione di impatto redatto dal Garante per la protezione dei dati personali.
7. In attuazione dell'art. 36 RGPD, il dipendente autorizzato al trattamento dei dati, prima di procedere al trattamento, se la valutazione d'impatto sulla protezione dei dati indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio, consulta preventivamente il Garante per la protezione dei dati personali.
8. Il Sindaco:
a) nomina i Responsabili dei Servizi quali destinatari di specifici compiti connessi al trattamento dei dati contenuti nelle banche dati, cartacee e informatiche, custodite presso gli stessi Uffici; in attuazione dell'art. 29 RGPD e dell'art. 2-quaterdecies, comma 2, D.Lgs. 196/03, dà nei decreti di nomina le necessarie istruzioni ai Responsabili di Servizio in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, al fornire istruzioni alle persone autorizzate al trattamento; delega ai Responsabili di Servizio la nomina dei dipendenti autorizzati al trattamento dei dati, l'individuazione di apposite istruzioni organizzative ed operative per il corretto, lecito, pertinente e sicuro trattamento dei dati, in attuazione dell'art. 29 e dell'art. 2–quaterdecies, comma 2 RGPD; i dipendenti autorizzati sono opportunamente istruiti e formati al trattamento con riferimento alla tutela del diritto alla riservatezza, nonché alle misure tecniche e organizzative da osservare per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati; delega ai Responsabili di Servizio la nomina dei Responsabili del trattamento nei casi in cui si faccia ricorso a soggetti esterni nell'ambito di contratti di affidamento di incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente; in attuazione dell'art. 28 RGPD, in questi casi il Responsabile di Servizio disciplina i trattamenti dai Responsabili del trattamento con contratto ovvero altro atto giuridico che vincoli il Responsabile al Comune;
a) nomina il Responsabile della Protezione dei Dati (DPO);
b) dispone periodiche verifiche, tramite il Responsabile della Protezione dei Dati (DPO), sul rispetto delle istruzioni date, anche con riguardo agli aspetti relativi alla sicurezza dei dati ed alla formazione ed istruzione dei dipendenti autorizzati al trattamento;
c) in attuazione dell'art. 33 RGPD, notifica al Garante per la protezione dei dati personali la violazione dei dati che rappresenti un rischio per i diritti e le libertà degli interessati, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;
d) in attuazione dell'art. 34 RGPD, comunica all'interessato, senza ingiustificato ritardo, la violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà dello stesso interessato;
e) assolve agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.
9. Nel caso di esercizio associato di funzioni e servizi che comportino il trattamento di dati personali, nonché nel caso in cui la gestione di funzioni o servizi sia affidata al Comune da parte di altre Amministrazioni ed organismi statali o regionali, se due o più Enti determinano congiuntamente le finalità ed i mezzi del trattamento si realizza la contitolarità di cui all'art. 26 RGPD. In questi casi, i contitolari determinano in modo trasparente, mediante un accordo interno, le

responsabilità di ciascuno in merito all'osservanza degli obblighi in materia di tutela del diritto alla riservatezza, con particolare riferimento all'esercizio dei diritti dell'interessato e alle rispettive funzioni, in relazione agli obblighi di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD. Il predetto accordo, il cui contenuto essenziale è messo a disposizione degli interessati, disciplina adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati; esso può individuare uno degli Enti contitolari del trattamento quale punto di contatto per gli interessati.

Art. 8 – I Responsabili di Servizio

1. In attuazione dell'art. 2-quaterdecies, comma 1, del D.Lgs. n. 196/2003, il Sindaco nomina i dipendenti incaricati della responsabilità di Servizio quali persone designate a specifici compiti connessi al trattamento dei dati personali e assegna loro i correlati poteri unitamente agli obblighi.
2. I Responsabili di Servizio:
a) nominano, su delega del Sindaco, i dipendenti comunali assegnati al Servizio autorizzati al trattamento dei dati personali;
b) nominano i Responsabili del trattamento nei casi in cui si fa ricorso a soggetti esterni per l'affidamento di incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente; i trattamenti da parte dei Responsabili sono disciplinati con contratto o altro atto giuridico che vincola il Responsabile del trattamento al Comune, ai sensi dell'art. 28 RGPD;
c) danno l'informativa agli interessati ai sensi degli artt. 12 e ss. RGPD, anche mediante adeguamento della modulistica resa disponibile dal Comune; le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici; se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata l'identità dell'interessato;
d) verificano e controllano che, nell'ambito del Servizio assegnato, il trattamento dei dati sia effettuato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicurare che i dati personali siano trattati in modo lecito, corretto e trasparente;
e) garantiscono che i dati personali siano raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità;
f) assicurano che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
g) adottano, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, tutte le misure tecniche ed organizzative, ivi comprese la pseudonimizzazione e la cifratura dei dati personali, necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del RGPD;
h) assistono il Sindaco al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;
i) assistono il Sindaco nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32 RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; se non vi possa provvedere immediatamente con i mezzi assegnati, il Responsabile del Servizio formula alla Giunta Comunale una proposta di adozione delle misure necessarie ed una stima dei costi preventivati per la realizzazione degli interventi proposti;
j) garantiscono l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; se non possa provvedere immediatamente con i mezzi assegnati, il Responsabile di Servizio formula alla Giunta Comunale una proposta di adozione delle misure necessarie ed una stima dei costi preventivati per la realizzazione degli interventi proposti;
k) assicurano l'adozione di procedure finalizzate a valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

l) informano senza ritardo il Sindaco in caso di violazione dei dati personali;
m) assistono il Sindaco nelle procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato, ai sensi degli artt. 33 e 34 del RGPD;
n) assistono il Sindaco e il Responsabile della Protezione dei Dati (DPO) nell'effettuazione della valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e nell'eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità all'art. 36 del RGPD;
o) sostituiscono il Sindaco, in attuazione dell'art. 30, paragrafo 1 e 2, del RGPD, nell'istituzione e aggiornamento del registro delle attività di trattamento, in base all'art. 17 del presente regolamento; con cadenza almeno annuale, ciascun dipendente autorizzato al trattamento istituisce nuove schede relative a nuove categorie di trattamento e aggiorna le schede del Registro dei trattamenti di propria competenza;
p) garantiscono che il Responsabile della Protezione dei Dati (DPO) designato dal Sindaco sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e riceva un adeguato affiancamento nell'esecuzione dei suoi compiti;
q) mettono a disposizione del Sindaco tutte le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Responsabile della Protezione dei Dati (DPO);
r) informano immediatamente il Sindaco se, a loro parere, un'istruzione data da quest'ultimo violi la normativa comunitaria o nazionale relativa alla protezione dei dati;
s) custodiscono e controllano i dati personali di competenza, affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
t) aggiornano sistematicamente la mappatura dei procedimenti amministrativi e censiscono periodicamente le banche dati di competenza del Servizio;
u) assicurano che il personale assegnato al Servizio si attenga, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantiscono che siano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
v) garantiscono la tempestiva emanazione di direttive ed ordini di servizio scritti ai dipendenti del Servizio autorizzati al trattamento previa se necessario consultazione del Responsabile della Protezione dei dati (DPO), necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
w) vigilano sul rispetto da parte dei dipendenti autorizzati al trattamento circa gli obblighi di corretta e lecita raccolta dei dati, di utilizzazione, di comunicazione nonché di diffusione degli stessi a mezzo pubblicazione all'Albo Pretorio On line ai sensi dell'art. 32, L. 69/2009 o nella Sezione Amministrazione Trasparente ai sensi del D.Lgs. 33/2013;
x) vigilano sul rispetto del diritto alla riservatezza nell'ambito dei procedimenti di accesso documentale, ai sensi e nei limiti degli artt. 22 e ss. L. 241/1990, o nei procedimenti di richiesta di accesso civico ai sensi dall'art. 5, comma 2 e dall'art. 5-bis, D.Lgs. 33/2013 di pertinenza del proprio Servizio; lo stesso obbligo di vigilanza si applica alle richieste di accesso dei Consiglieri Comunali ai sensi dell'art. 43, comma 2, del D.Lgs. 267/2000.

Art. 9 – I responsabili esterni del trattamento dei dati

1. Nei casi in cui il Comune, nell'ambito dell'affidamento di un incarico, un servizio, un lavoro, una fornitura, una collaborazione o una consulenza, affidi all'esterno un trattamento di dati per conto dell'Ente, il soggetto affidatario dell'incarico, del servizio, del lavoro, della fornitura, della collaborazione o della consulenza, sia esso persona fisica o persona giuridica, deve essere preventivamente individuato quale Responsabile del trattamento ai sensi dell'art. 28 RGPD.

2. In attuazione dell'art. 7, comma 9, lett. e) e dell'art. 8, comma 2, lett. a), del presente regolamento, l'obbligo di provvedere alla disciplina dei trattamenti da parte dei Responsabili, mediante contratto o altro atto giuridico, è affidato ai Responsabili di Servizio, che procedono, in base alle vigenti disposizioni in materia, all'affidamento di servizi, forniture, lavori, incarichi, consulenze e collaborazioni che comportino un trattamento di dati svolto dal soggetto affidatario per conto del Comune.

3. I Responsabili esterni del trattamento si obbligano a:

a) non ricorrere ad altro Responsabile senza previa autorizzazione scritta del Responsabile di Servizio;

b) non trasferire i dati personali del Comune verso un paese fuori UE senza previa autorizzazione scritta del Responsabile di Servizio**;**

c) verificare e controllare che, nell'ambito della propria organizzazione, il trattamento dei dati sia effettuato nel rispetto dei principi di cui all'art. 5 RGPD e, in particolare, assicurare che i dati personali siano trattati in modo lecito, corretto e trasparente; garantire altresì che, in caso di raccolta, i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;

d) assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

e) garantire che le persone che nell'ambito della propria organizzazione sono autorizzate al trattamento dei dati personali abbiano ricevuto una adeguata formazione con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati e abbiano un adeguato obbligo legale di riservatezza;

f) adottare, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, tutte le misure tecniche ed organizzative, ivi comprese la pseudonimizzazione e la cifratura dei dati personali, necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;

g) assistere il Sindaco con misure tecniche e organizzative adeguate al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;

h) assistere il Sindaco nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32 RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

i) garantire l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico;

j) assicurare l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

k) informare senza ritardo il Sindaco, in caso di violazione dei dati personali;

l) assistere il Sindaco nelle procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;

m)assistere il Sindaco nell'effettuazione della valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;

n) designare il proprio Responsabile della Protezione dei Dati (DPO) nei casi previsti dall'art. 37 del RGPD, pubblicare i suoi dati di contatto e comunicarli al Garante per la protezione dei dati personali e al Sindaco;

o) istituire ed aggiornare, in conformità alle disposizioni di cui all'art. 30, paragrafo 2, del RGPD, un registro, tenuto in forma scritta, di tutte le categorie di attività relative al trattamento svolte per conto del Comune;

p) garantire che il Responsabile della Protezione dei Dati (DPO) designato dal Comune sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
q) restituire al Comune, al momento della cessazione del contratto, incarico, fornitura, consulenza, collaborazione, oggetto di affidamento, tutti i dati personali trattati e a cancellare le copie esistenti, salvo il caso in cui la normativa europea o nazionale preveda la conservazione dei dati;
r) mettere a disposizione del Comune tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;
s) informare immediatamente il Sindaco qualora, a loro parere, un'istruzione data violi la normativa comunitaria o nazionale relativa alla protezione dei dati.

Art. 10 – I dipendenti del Comune autorizzati al trattamento dei dati

1. I dipendenti del Comune autorizzati al trattamento dei dati sono nominati con atto dal Responsabile di Servizio, su delega del Sindaco.
2. In attuazione dell'art. 7, comma 9, lett. f) del presente regolamento, i Responsabili di Servizio nominano i dipendenti autorizzati al trattamento dei dati, dando loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati, in attuazione dell'art. 29 RGPD e dell'art. 2-quaterdecies, D.Lgs. 196/03.
3. In attuazione dell'art. 8, comma 2, lett. b) del presente regolamento, ciascun Responsabile di Servizio, tenuto conto dei procedimenti amministrativi di competenza degli Uffici assegnati, del censimento delle banche dati cartacee e/o informatiche trattate dai singoli Uffici per la gestione dei procedimenti amministrativi di competenza, cura la formazione dei dipendenti autorizzati al trattamento dei dati con riferimento alla tutela del diritto alla riservatezza, nonché alle misure tecniche e organizzative da osservare per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati.
4. L'atto di nomina del Responsabile del Servizio contiene le istruzioni e le regole tecniche e operative che i dipendenti autorizzati al trattamento sono tenuti a seguire nelle operazioni di trattamento dei dati personali assegnate, l'indicazione dei loro obblighi e responsabilità con particolare riferimento a:
a. l'accesso alle banche dati informatiche;
b. la conservazione dei supporti informatici e/o cartacei contenenti dati personali;
c. la riservatezza ed il riserbo sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
d. la custodia ed il controllo dei dati personali affidati;
e. la conservazione dei dati in conformità alle misure di sicurezza adottate dall'Ente;
f. l'utilizzo della postazione di lavoro assegnata;
g. il collegamento ad Internet;
h. l'utilizzo dei supporti di memoria magnetici e ottici;
i. l'utilizzo della posta elettronica.
5. I dipendenti autorizzati sono tenuti alla riservatezza sui dati di cui siano venuti a conoscenza nell'esercizio delle funzioni istituzionali assegnate e provvedono al loro trattamento attenendosi scrupolosamente alle istruzioni date dal Responsabile del Servizio.
6. In attuazione dell'art. 5 RGPD, i dipendenti autorizzati devono assicurare che, nel corso del trattamento, i dati personali siano:
- trattati in modo lecito, corretto e trasparente;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione);

- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

7. All'atto di autorizzazione al trattamento è equiparato l'atto di assegnazione del dipendente al Servizio per il quale siano individuati analiticamente in forma scritta: l'ambito del trattamento consentito, i compiti e le funzioni connessi al trattamento assegnati al singolo dipendente; per effetto di tale disposizione, ogni dipendente assegnato al Servizio con atto di assegnazione che stabilisca l'ambito del trattamento consentito ed i compiti e le funzioni connessi al trattamento attribuiti è autorizzato al trattamento, ai sensi dell'art. 2-quaterdecies, comma 2, D.Lgs. 196/03.
8. I dipendenti autorizzati sono beneficiari di interventi formativi che prevedano richiami di aggiornamento periodici.

Art. 11 – Le persone non dipendenti del Comune autorizzate al trattamento dei dati

1. Le persone fisiche, non legate al Comune da un contratto di lavoro subordinato, che abbiano accesso ai dati personali trattati dagli Uffici per svolgere compiti di supporto agli stessi che comportino un trattamento di dati (ad esempio: i tirocinanti, i volontari, i collaboratori, tutti i soggetti che operano temporaneamente all'interno della struttura organizzativa del Comune), devono essere preventivamente autorizzate al trattamento, con atto formale del Responsabile del Servizio competente.
2. Le persone autorizzate sono soggette agli stessi obblighi cui sono sottoposti i dipendenti del Comune autorizzati al trattamento, in modo da garantire il pieno rispetto della tutela della riservatezza delle persone fisiche alle quali si riferiscono i dati oggetto di trattamento.
3. Le persone autorizzate sono beneficiarie di interventi formativi che prevedano richiami di aggiornamento periodici.

Art. 12 – Il responsabile della protezione dei dati

1. In attuazione dell'art. 37, paragrafi 5-6, RGPD, il Responsabile della protezione dei dati (DPO) è nominato dal Sindaco in funzione della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di dare corretto adempimento ai compiti di cui all'art. 39 RGPD.
2. La funzione di DPO può essere esercitata in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna al Comune, in tal caso è indispensabile che la persona fisica che opera quale DPO del Comune possieda tutti i requisiti richiesti dall'art. 37, paragrafo 5, RGPD e, in particolare, abbia maturato approfondita conoscenza della Pubblica Amministrazione e degli Enti Locali, della loro organizzazione, delle norme e procedure amministrative agli stessi applicabili.
3. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi, il DPO esterno è tenuto a procedere sistematicamente nell'aggiornamento della propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
4. Il DPO può essere individuato tra i dipendenti del Comune, in possesso di competenze e professionalità adeguate alla natura dell'incarico, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dei dati all'interno dell'organizzazione dell'Ente. Il Sindaco ed i Responsabili di Servizio provvedono affinché il DPO interno mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
5. In attuazione dell'art. 37, paragrafo 3, RGPD, è possibile l'affidamento dell'incarico di DPO ad un unico soggetto, anche esterno, designato da più Comuni, mediante esercizio associato della

funzione nelle forme previste dal D.Lgs. n. 267/2000.
6. Il DPO è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:
a) informare e fornire consulenza al Sindaco, ai Responsabili di Servizio e ai dipendenti autorizzati al trattamento, in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati personali;
b) partecipare alle riunioni di coordinamento dei Responsabili di Servizio che abbiano ad oggetto questioni inerenti alla protezione dei dati personali;
c) provvedere alla formazione dei Responsabili di Servizio e dei dipendenti autorizzati al trattamento, in merito agli obblighi derivanti dal RGPD in conformità alle disposizioni vigenti;
d) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati, nonché l'osservanza delle prassi adottate dai Responsabili di Servizio 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;
e) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'art. 35 RGPD; il Responsabile di Servizio si consulta con il DPO in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne o esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno, se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al RGPD;
f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per tale Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD ed effettuare, se del caso, consultazioni relativamente a ogni altra questione; a tali fini il nominativo del DPO è comunicato dal Comune al Garante;
g) tenere il registro delle attività dei trattamenti di cui al successivo art. 17;
h) fornire supporto tecnico-giuridico al Sindaco in relazione ai trattamenti operati sui social media e/o sui social network.
7. I Responsabili di Servizio assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali; a tal fine:
a) mettono a disposizione del DPO le risorse umane e materiali necessarie a consentirgli l'ottimale svolgimento dei compiti e delle funzioni assegnate, garantendogli l'accesso ai dati personali ed ai trattamenti;
b) garantiscono al DPO il supporto dell'Amministratore di Sistema Informatico del Comune per la soluzione delle problematiche relative alla protezione dei dati personali che abbiano un'incidenza diretta o indiretta sulle attività di trattamento effettuate con l'ausilio di strumenti informatici;
c) forniscono al DPO le informazioni in merito al trattamento dei dati personali e alle misure di sicurezza adottate dal Comune, al fine di consentire allo stesso DPO di fornire al Comune una consulenza funzionale alle problematiche oggetto di analisi; il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante; nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal DPO, è necessario che il Sindaco o i Responsabili di Servizio motivino tale decisione;
d) consultano tempestivamente il DPO nel caso in cui si verifichi una violazione dei dati o altro incidente in grado di avere rilevanza sui dati personali trattati dal Comune.
8. Nello svolgimento dei compiti affidatigli il DPO deve considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
9. La funzione di DPO è incompatibile con le seguenti:
a) Responsabile per la prevenzione della corruzione e per la trasparenza;
b) Responsabile di Servizio;
c) Sindaco.

10. Il DPO opera in posizione di autonomia nello svolgimento dei compiti attribuiti, non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati.
11. Il DPO non può essere rimosso dall'incarico dal Sindaco o penalizzato o altrimenti ostacolato nell'adempimento dei propri compiti.
12. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Sindaco e ai Responsabili di Servizio.

CAPO III – PRINCIPI

Art. 13 - Principi e responsabilizzazione

1. Sono integralmente recepiti nell'organizzazione interna del Comune i principi del RGPD, per effetto dei quali i dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
b) 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 considerato incompatibile con le finalità iniziali ("limitazione della finalità");
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
e) 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'art. 89, paragrafo 1, RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");
f) 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 ("integrità e riservatezza");
g) configurati riducendo 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 ("necessità").
2. I Responsabile di Servizio sono responsabili del rispetto dei principi predetti e devono essere in grado di comprovarne il rispetto, in base al principio di "responsabilizzazione".

Art. 14 - Condizioni per il consenso

1. Fermi restando i casi in cui il trattamento sia effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune, o per i dati di cui agli artt. 9 e 10 RGPD nelle ipotesi in cui il trattamento sia necessario per motivi di interesse pubblico rilevante (nei quali può essere effettuato senza il consenso dell'interessato), se il trattamento dei dati personali, per una o più specifiche finalità, sia subordinato al consenso dell'interessato, si applica la disciplina di cui all'art. 7 RGPD, la quale prevede che:

a) il dipendente autorizzato al trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
b) se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro;
c) l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento; la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca; prima di esprimere il proprio consenso, l'interessato deve essere informato di ciò; il consenso è revocato con la stessa facilità con cui è accordato;
d) nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto;
e) per i dati sensibili di cui all'art. 9, RGPD, il consenso deve essere esplicito e prestato in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;
f) il consenso deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto;
g) deve essere manifestato attraverso dichiarazione o azione positiva inequivocabile.
2. Se il trattamento è basato sul consenso, il consenso deve essere reso da parte dell'interessato attraverso la compilazione di apposita modulistica, resa disponibile dal dipendente autorizzato al trattamento, previa consegna e presa d'atto dell'informativa di cui al successivo art. 15.
3. In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.
4. La manifestazione del consenso ad opera dell'interessato deve essere resa al momento del primo accesso ai servizi o prestazioni ed è valida ed efficace fino alla revoca della stessa.
5. Il consenso è registrato nel registro delle attività di trattamento.

Art. 15 – Informativa all'interessato

1. Ciascun Responsabile di Servizio assicura, avvalendosi dei dipendenti autorizzati al trattamento che, al momento della raccolta dei dati personali, agli interessati sia fornita apposita informativa secondo le modalità previste dall'art. 13, RGPD, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.
2. L'informativa è fornita per iscritto, anche in formato elettronico, soprattutto nel contesto di servizi resi in modalità online.
3. L'informativa può essere fornita con le seguenti modalità:
a) attraverso apposita modulistica resa disponibile agli interessati;
b) attraverso avvisi agevolmente accessibili al pubblico diffusi attraverso pubblicazione sul sito istituzionale del Comune;
c) attraverso apposita avvertenza inserita nei contratti o nelle lettere di affidamento di incarichi con i quali sono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti e di altri soggetti chiamati a prestare la loro attività per conto del Comune;
d) in sede di pubblicazione dei bandi, degli avvisi, delle lettere d'invito.
4. L'informativa deve riportare il seguente contenuto minimo:
a) l'identità ed i dati di contatto del Sindaco;
b) i dati di contatto del DPO;

c) le indicazioni circa le finalità del trattamento;
d) la base giuridica del trattamento;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) l'eventuale intenzione del Comune di trasferire i dati personali ad un Paese terzo o a un'organizzazione internazionale;
g) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
h) l'esistenza del diritto dell'interessato di chiedere al Comune l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
i) qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualunque momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
j) l'indicazione sul fatto che la comunicazione dei dati personali è un obbligo legale o contrattuale, o un requisito necessario per la conclusione di un contratto, o se l'interessato abbia l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione dei dati;
k) il diritto di proporre reclamo al Garante per la protezione dei dati personali;
l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.
5. Se il Comune intende trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni circa tale diversa finalità e ogni ulteriore informazione ritenuta utile.
6. Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato, ciascun Responsabile di Servizio, avvalendosi dei dipendenti autorizzati al trattamento, fornisce all'interessato le seguenti informazioni:
a) l'identità ed i dati di contatto del Sindaco;
b) i dati di contatto del DPO;
c) le indicazioni circa le finalità del trattamento;
d) la base giuridica del trattamento;
e) le categorie di dati personali trattati;
f) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
g) l'eventuale intenzione del Comune di trasferire i dati personali ad un Paese terzo o a un'organizzazione internazionale;
h) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
i) l'esistenza del diritto dell'interessato di chiedere al Comune l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
j) qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualunque momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
k) il diritto di proporre reclamo al Garante per la protezione dei dati personali;
l) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
m) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.
7. L'informativa, nei casi di cui al precedente comma 6, deve essere fornita entro un termine ragionevole dall'ottenimento dei dati personali e, al più tardi, entro un mese. Nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, l'informativa deve essere fornita al più tardi al momento della prima comunicazione all'interessato. Nel caso sia prevista la

comunicazione ad altro destinatario, l'informativa deve essere fornita non oltre la prima comunicazione dei dati personali.

Art. 16 – Formazione e sensibilizzazione del personale

1. 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 Sindaco promuove all'interno del Comune ogni iniziativa di formazione che possa consolidare la consapevolezza del valore del diritto alla riservatezza dei dati, al fine di migliorare la qualità dei servizi resi nei confronti degli interessati; a tale riguardo, il presente regolamento riconosce nell'attività di formazione ed informazione resa ai Responsabili di Servizio un ruolo essenziale per la responsabilizzazione e la sensibilizzazione dei diversi soggetti coinvolti nel trattamento di dati personali.
2. Al fine di assicurare la conoscenza capillare delle disposizioni contenute nel RGPD e nel presente regolamento, al momento dell'ingresso in servizio è consegnata ad ogni dipendente una specifica comunicazione, che richiama l'apposita clausola inserita nel contratto di lavoro, contenente i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale; il dipendente si impegna ad acquisire copia del presente regolamento, prenderne visione ed attenersi alle sue prescrizioni.
3. Il presente regolamento è pubblicato sul sito istituzionale del Comune nella Sezione Amministrazione Trasparente, Sotto Sezione di I Livello "Altri Contenuti", Sotto Sezione di II Livello "Privacy".
4. I Responsabili di Servizio organizzano, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, con cadenza annuale, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione dei rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso illegittimo ai dati conservati e trattati dai dipendenti del Comune. Gli interventi formativi ed informativi sono finalizzati a rendere informati i Responsabili di Servizio ed i dipendenti autorizzati al trattamento di dati personali delle misure di sicurezza adottate dal Comune ai sensi dell'art. 32 RGPD al fine di assicurare l'integrità, la riservatezza, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
5. La formazione in materia di tutela del diritto alla riservatezza e prevenzione dei rischi di violazione dei dati personali è integrata con la formazione in tema di trasparenza e di diritto di accesso, con particolare riguardo al corretto bilanciamento tra il diritto alla protezione dei dati personali e le contrapposte esigenze di trasparenza dell'azione amministrativa, nonché di diritto di accesso ai documenti amministrativi di cui agli artt. 22 e ss. L. 241/90 e di diritto di accesso civico generalizzato di cui all'art. 5, comma 2, D.Lgs. 33/2013, nei diversi ambiti in cui opera il Comune.
6. La partecipazione dei dipendenti agli interventi formativi è considerata quale presupposto essenziale per il corretto trattamento dei dati personali e criterio di misurazione e valutazione della performance organizzativa ed individuale.

Art. 17 - Registro delle attività di trattamento

1. In attuazione dell'art. 30, paragrafo 1, del RGPD, ciascun Responsabile di Servizio istituisce, in forma scritta, un registro delle attività di trattamento e di tutte le categorie di attività relative al trattamento, svolte sotto la propria responsabilità.
2. Il registro delle attività di trattamento reca almeno le seguenti informazioni:
a) il nome e i dati di contatto del Comune, del legale rappresentante del Comune, del Responsabile della Protezione dei Dati (RPD);
b) le finalità del trattamento;
c) le categorie dei trattamenti effettuati da parte del Servizio;
d) la descrizione delle categorie di interessati e delle categorie di dati personali;

e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
f) se applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 RGPD, la documentazione delle garanzie adeguate;
g) se possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
h) il richiamo alle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1, RGPD.
3. Il Comune delega la vigilanza sulla corretta tenuta del registro delle attività di trattamento al Responsabile per la Protezione dei Dati (DPO). Ciascun Responsabile di Servizio deve fornire prontamente e correttamente al Responsabile per la Protezione dei Dati ogni elemento, dato e informazione necessari alla regolare formazione, tenuta e all'aggiornamento del registro delle attività di trattamento.
4. Su richiesta, il Responsabile del Servizio mette il registro a disposizione del Garante.
5. Il registro è tenuto in forma scritta, anche in formato elettronico e deve essere periodicamente aggiornato, con cadenza almeno annuale e, in ogni caso, ogniqualvolta vi siano delle modifiche che richiedono la loro trascrizione nel registro dei trattamenti (modalità di trattamento, finalità, categorie di dati, categorie di interessati, ecc.).
6. Il registro delle attività dei trattamenti è adottato con provvedimento del Responsabile del Servizio e, successivamente, con cadenza annuale, con analogo provvedimento sono adottate le revisioni del registro delle attività dei trattamenti che danno conto delle eventuali modifiche/integrazioni e novità intercorse con riferimento alle categorie di dati trattati, alle modalità di trattamento, alle finalità, alle categorie di interessati, nonché alle misure di sicurezza tecniche ed organizzative di cui all'art. 32 RGPD.

CAPO IV – PUBBLICITA' E DIFFUSIONE SUL WEB DI DOCUMENTI CONTENENTI DATI PERSONALI

Art. 18 - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. I Responsabili di Servizio ed i dipendenti autorizzati al trattamento dei dati, al momento della pubblicazione sul sito istituzionale del Comune, nelle Sezioni "Albo pretorio on-line" e "Amministrazione Trasparente", di dati personali contenuti in atti e provvedimenti amministrativi per i quali un'espressa previsione normativa ne preveda l'obbligo di pubblicazione, assicurano il rispetto dei principi di pertinenza e minimizzazione di cui all'art. 5, paragrafo 1, lett. c), RGPD.
2. La pubblicazione di un atto sul sito istituzionale del Comune costituisce un'operazione di diffusione dei dati personali in esso contenuti; detta circostanza impone al dipendente autorizzato al trattamento di valutare preventivamente, di volta in volta, quali siano le informazioni personali la conoscenza delle quali sia realmente rilevante rispetto alle specifiche finalità perseguite con la pubblicazione medesima.
A questo fine, si mettono in evidenza le regole seguenti:
- la diffusione di dati personali, ossia il dare conoscenza dei dati personali a soggetti indeterminati mediante la pubblicazione sul sito istituzionale da parte dei soggetti pubblici, è ammessa unicamente se la stessa è prevista da una specifica norma di legge o di regolamento (art. 2-ter, comma 1, D.Lgs. 196/03);
- se il dipendente autorizzato al trattamento riscontra l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento sul sito web istituzionale, deve selezionare i dati personali da inserire nel documento, verificando caso per caso se ricorrano i presupposti per l'oscuramento di determinate informazioni;

- è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria ("principio di pertinenza e minimizzazione" art. 5, paragrafo 1, lett. c), RGPD);
- è sempre vietata la diffusione di dati idonei a rivelare lo stato di salute e la vita sessuale (art. 2-septies, comma 8, D.Lgs. 196/03 e art. 7-bis, comma 6, D.Lgs. 33/2013), nonché la situazione di disagio economico sociale degli interessati (art. 26, comma 4, D.Lgs. 33/2013).

3. Una volta trascorso l'arco temporale previsto dalle singole norme per la pubblicazione degli atti e dei documenti sul sito web del Comune, il Responsabile del procedimento provvede senza indugio alla loro eliminazione.

CAPO V - SICUREZZA DEI DATI PERSONALI

Art. 19 – Sicurezza del trattamento

1. Ciascun Responsabile di Servizio, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, del campo di applicazione, del contesto e delle finalità del trattamento, del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, che comprendono:
- 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 che trattano 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.

2. Costituiscono misure tecniche ed organizzative che possono essere adottate da ciascun Responsabile di Servizio, previa consultazione con il Responsabile del Trattamento dei Dati (DPO) e con l'Amministratore di Sistema dell'Ente:
- sistemi di autenticazione;
- sistemi di autorizzazione;
- sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio;
- sistemi di rilevazione di intrusione;
- sistemi di sorveglianza;
- sistemi di protezione con videosorveglianza;
- registrazione accessi;
- porte, armadi e contenitori dotati di serrature e ignifughi;
- sistemi di copiatura e conservazione di archivi elettronici;
- ulteriori misure per ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico.

3. In attuazione dell'art. 32 RGPD, la conformità del trattamento dei dati al RGDP è dimostrata attraverso l'adozione delle misure di sicurezza adeguate al rischio, o attraverso l'adesione a codici di condotta approvati o ad altri meccanismi di certificazione approvati.

Art. 20 -Valutazioni d'impatto sulla protezione dei dati

1. La valutazione d'impatto sulla protezione dei dati (di seguito "DPIA") è un procedimento finalizzato a descrivere il trattamento, valutarne la necessità e la proporzionalità, contribuire a

gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
2. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ciascun Responsabile di Servizio, prima di effettuare il trattamento, deve disporre una valutazione dell'impatto del trattamento (DPIA) ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
3. Ai fini della decisione di effettuare o meno la DPIA, ciascun Responsabile di Servizio tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione, redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, paragrafi 4-5-6, RGPD; a questo proposito si richiama integralmente l'Allegato 1 al Provvedimento del Garante Privacy n. 467 dell 11.10.2018 ed i successivi provvedimenti, contenenti gli elenchi delle tipologie di trattamenti soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto.
4. Ciascun Responsabile di Servizio, prima di disporre una DPIA, si consulta con il Responsabile della Protezione dei Dati (DPO), che fornisce parere in merito e ne sorveglia lo svolgimento ai sensi dell'art. 35 RGPD.
5. L'Amministratore di Sistema dà supporto al Responsabile di Servizio e al Responsabile della Protezione dei Dati (DPO) per lo svolgimento della DPIA.
6. La DPIA non è necessaria nei seguenti casi:
- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, RGPD;
- 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;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se 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. La DPIA condotta prima di dar luogo al trattamento deve contenere almeno i seguenti elementi:
a) la descrizione sistematica del contesto, dei trattamenti previsti e delle finalità del trattamento, i dati personali oggetto del trattamento, i destinatari, il periodo previsto di conservazione dei dati, la descrizione funzionale del trattamento, gli strumenti coinvolti nel trattamento (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) la valutazione dei rischi per i diritti e le libertà degli interessati, con particolare riguardo alla probabilità e alla gravità dei rischi rilevati;
d) l'individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento al RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8. 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 trattamento.

Art. 21 - Consultazione preventiva

1. Il Responsabile di Servizio, prima di procedere al trattamento dei dati, consulta, tramite il DPO, il Garante della Privacy, se la valutazione d'impatto sulla protezione dei dati ha evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate per attenuare il rischio.

Art. 22 - Notifica di una violazione dei dati personali

1. Per violazione dei dati personali s'intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.
2. Il Responsabile di Servizio, se ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, notifica la violazione al Garante Privacy entro 72 ore e comunque senza ritardo.
3. Il Responsabile di Servizio è obbligato ad informare il Sindaco, senza ritardo, dopo essere venuto a conoscenza della violazione di dati personali.
4. La notifica al Garante Privacy deve:
a) descrivere la natura della violazione dei dati personali, compresi se possibile le categorie e il numero approssimativo di interessati in questione, le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati (RPD) presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Comune per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
5. Se non sia possibile fornire contestualmente le informazioni di cui al precedente comma 4, dette informazioni possono essere fornite in fasi successive senza ulteriore ritardo.
6. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione sono quelli descritti al considerando 75 del RGPD, che si riporta integralmente: "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*."
7. Il Responsabile di Servizio deve documentare le violazioni di dati personali subite, anche se non comunicate all'Autorità di controllo, le circostanze ad esse relative, le conseguenze e i provvedimenti adottati per porvi rimedio; tale documentazione, da conservarsi diligentemente, deve essere esibita, su richiesta del Garante Privacy, al fine della verifica del rispetto delle disposizioni di cui all'art. 33 RGPD.

Art. 23 - Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione di dati personali è suscettibile di presentare un rischio elevato per i diritti e

le libertà delle persone fisiche, il Responsabile di Servizio comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni:

- il nome e i dati di contatto del Responsabile della Protezione dei Dati (RPD) presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del Comune per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

3. Non è richiesta la comunicazione all'interessato nei casi in cui:
a) il Comune ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure sono state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Comune ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati; in tal caso si procede ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il Comune non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante Privacy può richiedere che vi provveda, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato o può decidere che una delle condizioni di cui al precedente comma 3, lett. a), b) e c) sia soddisfatta.

Art. 24 – Rinvio - esecutività

1. Per quanto non previsto dal presente regolamento, si rinvia al Regolamento UE 2016/679, al D.Lgs. 196/2003, alle Linee guida ed ai provvedimenti del Garante Privacy, alle Linee Guida del Comitato europeo per la protezione dei dati personali.
2. Il presente regolamento sarà aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.