COMUNE DI PASTRENGO

REGOLAMENTO GENERALE SULL'ORDINAMENTO DEGLI UFFICI E DEI SERVIZI

DISPOSIZIONI GENERALI

ART. 1 - DISPOSIZIONI GENERALI

Per ordinamento generale degli uffici e dei servizi si deve intendere l'insieme di provvedimenti di natura organizzativa che regolano il funzionamento dell'ente.

Gli atti organizzativi dell'ordinamento degli uffici e dei servizi costituiscono un sistema, e pertanto devono essere coordinati fra loro.

Il presente regolamento costituisce il quadro entro cui devono inserirsi ed a cui devono adeguarsi, gli altri atti organizzativi comunali.

Gli atti integrativi possono essere espressi come appendici al presente o come atti autonomi (ma coordinati).

Tutti gli atti dell'ordinamento generale degli uffici e dei servizi devono essere raggruppati in una raccolta di facile consultazione, anche ai fini della pubblicazione e del rispetto del principio della trasparenza.

Gli atti ed i provvedimenti costituenti l'ordinamento generale degli uffici devono essere costantemente aggiornati alle modifiche normative e/o del modello organizzativo.

In caso di modifiche all'ordinamento generale degli uffici e dei servizi e/o degli atti integrativi deve sempre seguire l'approvazione di un testo coordinato con le modifiche.[1]

[1] La disposizione serve a garantire il rispetto del principio di trasparenza.

Art. 2 - PRINCIPI GENERALI

L'ordinamento degli uffici e dei servizi si ispira ai seguenti principi e criteri che costituiscono anche strumento interpretativo delle disposizioni normative in esso contenute.

2.1 Principi generali fissati dall'ordinamento giuridico

Il sistema organizzativo del Comune di Pastrengo deve rispettare le regole di funzionamento stabilite dall'ordinamento giuridico per gli enti locali.

2.2 Principio della distinzione fra attività di indirizzo e controllo ed attività di gestione

La distinzione fra l'attività di indirizzo e controllo di competenza degli organi politici e l'attività di gestione, si esplica attraverso l'adozione ed approvazione di documenti programmatici da parte degli organi di governo.

Oltre ai documenti programmatici espressamente previsti dal quadro normativo di riferimento (PIAO, DUP, PEG, etc.) l'attività di indirizzo può essere esercitata anche attraverso singoli atti / provvedimenti di indirizzo approvati dalla Giunta e/o adottati dal Sindaco.

Gli indirizzi di natura politica vanno prontamente attuati dagli organi gestionali. La mancata attuazione degli atti programmatici o il mancato rispetto alle indicazioni del Sindaco, va valutato a livello di performance e/o come violazione disciplinare in base alla normativa vigente.

E' possibile il conferimento di poteri gestionali a componenti degli organi di governo ai sensi dell'articolo 53, comma 23, della l. n. 388/2000[2]

L'attività di controllo, da parte del Sindaco (in qualità di legale rappresentante dell'ente) comporta il potere di accesso a tutti i documenti amministrativi sia cartacei che telematici, nonché a tutti gli ambienti di proprietà o sotto controllo dell'ente comune.

[2] Il Comune di Pastrengo è un Comune con popolazione inferiore ai 5000 abitanti

2.3 Principio del risultato

Pur nel rispetto dei principi di legalità, correttezza e trasparenza, il principio del risultato deve essere considerato prioritario e va inteso nel senso di *privilegiare l'effettivo e tempestivo conseguimento degli obiettivi dell'azione pubblica, escludendo che la stessa sia vanificata da vuoti formalismi ed in tutti quei casi in cui non si rinvengano obiettive ragioni che ostino al suo espletamento*[3].

La mancata erogazione dei servizi all'utenza per ragioni formali potrà dar vita a sanzioni per interruzione di pubblico servizio e/o omissione di atti di ufficio, in base alla normativa vigente.

2.4 Principio della flessibilità ed adattabilità operativa

Pur nel rispetto del principio che il dipendente deve essere adibito alle mansioni per cui è assunto, e che deve svolgere i compiti e le mansioni declinate nel contratto individuale di lavoro, non costituisce esercizio di mansioni superiori o demansionamento lo svolgimento di compiti e mansioni, non prevalenti, appartenenti alla categoria professionale superiore o inferiore rispetto a quella dell'inquadramento. In ogni caso prevale il principio del risultato.

L'adeguamento alle modifiche organizzative costituisce obbligo contrattuale. Il mancato adeguamento comporta quindi una sanzione disciplinare, mentre il pronto adeguamento garantisce una valutazione positiva in base al sistema di valutazione vigente (*vedi principio premialità e merito*).

2.5 Principio della temporaneità e revocabilità degli incarichi

Tutti gli incarichi (di copertura di ruoli organizzativi) sono soggetti al principio della temporaneità e revocabilità.

[3] TAR Napoli, 15.01.2024 n. 377

2.6 Principio della fiducia

Il principio della fiducia, e quindi delle scelte e valutazioni discrezionali, va correlato con il principio del risultato.

2.7 Principio della digitalizzazione

L'organizzazione dell'ente e le relative procedure, compresa la conservazione dei documenti, deve essere improntata ai principi della digitalizzazione e dell'interscambiabilità dei dati anche per realizzare il (successivo) principio dell'once only.

Il mancato rispetto del principio comporta la decurtazione della retribuzione di risultato.

2.8 Principio dell'autocertificazione e dell'once only

I documenti attestanti atti, fatti, qualità e stati soggettivi, necessari per l'istruttoria dei diversi procedimenti amministrativi, sono acquisiti d'ufficio quando sono in possesso dell'amministrazione procedente, ovvero sono detenuti, istituzionalmente, da altre pubbliche amministrazioni. L'amministrazione procedente può richiedere agli interessati i soli elementi necessari per la ricerca dei documenti.[4]

I responsabili dei procedimenti non devono chiedere ai cittadini e alle imprese informazioni già fornite, e devono dare accesso ai loro fascicoli digitali e devono rendere disponibili a livello transfrontaliero i servizi pubblici rilevanti.[5]

La violazione del principio costituisce illecito disciplinare e/o comporta la decurtazione della retribuzione di risultato.

2.9 Macro e micro organizzazione

Gli atti di macro organizzazione sono adottati dagli organi di governo e non sono sindacabili se non per irragionevolezza.

Gli atti di micro organizzazione sono adottati dagli organi di gestione e sono adottati con i poteri del privato datore di lavoro

[4] Art. 18.2 legge 241/90

[5] Piano triennale dell'informatica AGID 2022- 2024. Le linee guida AGID emesse ai sensi dell'art. 71 del CAD sono vincolanti erga omnes Cons. St., comm. spec., 10 ottobre 2017, n. 2122

2.10 Organizzazione della struttura per aree di risultato o per la gestione (integrata) dei servizi e non per competenze professionali specialistiche

L'articolazione organizzativa dell'ente deve essere progettata ed interpretata nel senso che le diverse unità organizzative in cui è articolato l'ente devono essere responsabili di un risultato, come ad esempio l'erogazione integrale ed integrata di un servizio, e non solo di una corretta prestazione professionale da parte dei dipendenti in essa incardinati.

In ogni caso la competenza all'adozione dei provvedimenti amministrativi spetta all'unità organizzativa a cui sono attribuite le risorse economiche o le competenze prevalenti.

In caso di conflitto (positivo o negativo di competenza) decide il sindaco sentito il segretario comunale.[6]

2.11 Assunzioni e dotazioni organiche

Le procedure di assunzioni del personale a tempo determinato, indeterminato o a contratto, entro e fuori dotazione organica devono rispettare i principi generali di trasparenza ma devono essere improntate alla maggiore celerità possibile.

2.12 Trasparenza

L'azione amministrativa deve essere improntata al principio della trasparenza.

Costituisce obiettivo primario la corretta gestione e rispetto degli obblighi in tema di trasparenza (d.lgs 33/2013)

2.13 Principio della premialità e del merito

Il ciclo della performance, la conseguente valutazione dei risultati e l'erogazione dei premi, deve essere improntata al principio del merito.

Il sistema di valutazione ed il processo di valutazione devono prevedere meccanismi di confronto che coinvolgano anche il sindaco.

---

[6] L'affidamento del potere decisionale al sindaco è giustificata dal principio che nei comuni inferiori ai 5000 abitanti agli organi di governo possono essere affidati compiti gestionali.

2.14 Principio di soddisfazione dell'utenza

L'attività ammnistrativa deve essere improntata alla massima soddisfazione dell'utenza.

La mancata erogazione di servizi all'utenza senza giustificati motivi o per vuoti formalismi costituisce illecito disciplinare, secondo la normativa vigente.

ART. 3 - DEFINIZIONI

3.1 Unità organizzativa

Per Unità organizzativa si deve intendere un'articolazione dell'organizzazione generale dell'ente a cui è attribuita una "missione", la competenza a svolgere funzioni, erogare servizi, gestire procedimenti amministrativi.

Il funzionamento dell'unità organizzativa è garantito dai ruoli organizzativi in essa presenti.

3.2 Ruolo organizzativo

Per ruolo organizzativo si deve intendere l'insieme di poteri, compiti e responsabilità attribuiti ad un soggetto in possesso di idoneo profilo professionale.

3.3 Profilo professionale

Per profilo professionale deve intendersi l'insieme delle conoscenze, competenze e capacità che permettono di ricoprire uno o più ruoli organizzativi.

3.4 Procedimento amministrativo

Per procedimento amministrativo si deve intendere una serie di atti e di attività finalizzati all'adozione del provvedimento amministrativo che rappresenta l'atto finale della sequenza, attraverso cui la Pubblica Amministrazione manifesta la propria volontà.

3.5 Output

Per output si deve intendere "*il prodotto finale*" (o i prodotti finali) erogati dall'unità organizzativa competente che può essere un provvedimento amministrativo [7], un'azione o un'attività.

ASSETTO MACRO STRUTTURALE

ART. 4 - ATTI DI MACRO ORGANIZZAZIONE E DI MICRO ORGANIZZAZIONE

Sono atti di macro - organizzazione i provvedimenti con cui si assumono decisioni sul modello organizzativo dell'ente, sulla sua articolazione organizzativa, sulle competenze delle diverse unità organizzative, sulla composizione delle dotazioni organiche, sull'attribuzione del personale alle diverse unità organizzative di massimo livello, sulle regole di conferimento e revoca dei diversi ruoli organizzativi.

Gli atti di macro-organizzazione sono di competenza degli organi di governo e non sono sindacabili se non per irragionevolezza.

Sono atti di micro-organizzazione gli atti che incidono direttamente sui rapporti di lavoro, e sono assunti dai dirigenti (funzionali) [8] con i poteri del privato datore di lavoro.

ART. 5 - ASSETTO MACROSTRUTTURALE

La macrostruttura definisce i livelli di articolazione organizzativa dell'ente.

Il Comune di Pastrengo può essere articolato in:

a) Aree (*unità organizzative obbligatorie*)

b) Uffici (*unità organizzative eventuali*)

c) Unità di progetto (*unità organizzative eventuali*)

La macrostruttura dell'ente è approvata con atto della Giunta Comunale che definisce, anche con atti separati:

- l'articolazione dell'ente in aree ed eventualmente in uffici
- le competenze ed i servizi attribuiti alle singole unità organizzative;

---

[7] L'output è normalmente un provvedimento amministrativo emesso a seguito di istruttoria (permesso di costruire) ma può essere anche un'azione e/o un'attività materiale; gli output delle diverse unità organizzative sono definite in apposito atto organizzativo

[8] Il Comune di Pastrengo non è dotato di dirigenti per cui per dirigenti dell'ente si devono intendere dipendenti, di norma di livello apicale, incaricati di ricoprire ruoli organizzativi che comportano l'assunzione di decisioni gestionali.

- gli output delle diverse unità organizzative.

ART. 6 - AREE

Le Aree sono le unità organizzativa di massima dimensione deputate alla gestione integrata dei servizi ad essa attribuiti.

Per gestione integrata dei servizi si deve intendere una gestione orientata al risultato, nel senso che il personale assegnato non è responsabile solo di una corretta prestazione professionale ma dell'effettiva erogazione del servizio, inteso come *output* dell'area.

La mancata o la ritardata erogazione dei servizi attribuiti all'area (output) per motivi strumentali e/o formali può costituire interruzione di pubblico servizio.

I servizi attribuiti all'area, ed eventualmente gli output, sono indicati nell'atto di approvazione della macrostruttura dell'ente o in atti integrativi ad essa connessi.

ART. 7 - UFFICI

Gli uffici sono articolazioni organizzative di secondo livello.

L'eventuale sub articolazione dell'Area in uffici è di competenza della Giunta comunale.

ART 8 - UNITA' DI PROGETTO

Le Unità di progetto sono unità organizzative eventuali e temporanee.

Le Unità di progetto sono costituite con atto della Giunta Comunale quando la definizione e l'attuazione di un obiettivo coinvolgono competenze appartenenti ad aree differenti, o quando l'obiettivo è particolarmente importante e/o strategico e necessita di risorse dedicate.

L'Unità di progetto può essere costituita anche da un solo dipendente o da un incaricato a contratto.

ART. 9 - UFFICI ALLE DIRETTE DIPENDENZE DEGLI ORGANI DI GOVERNO

La Giunta comunale, con propria deliberazione, può costituire uffici posti alle dirette dipendenze del Sindaco, della Giunta e/o degli Assessori, per l'esercizio delle funzioni di indirizzo e controllo loro attribuite dalla legge.

Il provvedimento di costituzione ne individua la composizione e l'inserimento nello schema organizzativo del Comune.

Il personale degli Uffici di supporto agli organi di direzione politica può essere costituito da:

a) personale dell'Ente, trasferito attraverso processi di mobilità interna;

b) personale in servizio presso altre P.A. assunto con contratto a tempo determinato che a seguito dell'incarico è collocato in aspettativa senza assegni;

c) personale con incarichi a contratto;

d) collaboratori esterni ad alta specializzazione con incarichi a contratto.

Gli incarichi sono affidati con proprio atto dal Sindaco che può emettere anche i provvedimenti presupposti e conseguenti all'affidamento dell'incarico.

RUOLI ORGANIZZATIVI

ART. 10 - DEFINIZIONE DI RUOLO ORGANIZZATIVO

Per ruolo organizzativo si deve intendere l'insieme di poteri, compiti e responsabilità attribuiti ad un soggetto in possesso di idoneo profilo professionale.

L'attribuzione e la revoca degli incarichi di copertura dei ruoli organizzativi è definito con il presente regolamento o con atti integrativi

ART 11 - RUOLI ORGANIZZATIVI DI ELEVATA QUALIFICAZIONE

I ruoli organizzativi di E.Q. possono essere di due tipologie:

a) *posizioni di EQ di tipo gestionale*, e cioè posizioni di responsabilità di direzione di unità organizzative di particolare complessità, caratterizzate da elevato grado di autonomia gestionale e organizzativa (*ad esempio: responsabile di area; responsabile di ufficio; responsabile di unità di progetto*)

b) *posizioni di EQ di tipo specialistico*, e cioè posizioni lavorative con contenuti di alta professionalità, comprese quelle comportanti l'iscrizione ad albi professionali, richiedenti elevata competenza specialistica acquisita attraverso titoli formali di livello universitario del sistema educativo e di istruzione oppure attraverso

consolidate e rilevanti esperienze lavorative in posizioni ad elevata qualificazione professionale o di responsabilità, risultanti dal curriculum.

I ruoli organizzativi di elevata qualificazione, d'ora in poi EQ sono individuati dall'ente con apposito provvedimento

Gli incarichi di copertura dei ruoli di EQ, afferenti alle suddette posizioni di lavoro possono essere affidati a personale dipendente inquadrato nell'area dei Funzionari e dell'Elevata a personale acquisito dall'esterno con incarichi a contratto ed inquadrato nella medesima area, eccezionalmente e temporaneamente possono essere affidate anche a personale dipendente inquadrato nell'area degli istruttori.

ART. 12 - SEGRETARIO COMUNALE

Il *Segretario comunale*:

a) svolge compiti di collaborazione e funzioni di assistenza giuridico-amministrativa nei confronti degli organi dell'ente in ordine alla conformità dell'azione amministrativa alle leggi, allo statuto ed ai regolamenti;
b) sovrintende allo svolgimento delle funzioni dei dirigenti e ne coordina l'attività, Il segretario

inoltre:

c) partecipa con funzioni consultive, referenti e di assistenza alle riunioni del consiglio e della giunta e ne cura la verbalizzazione;
d) esprime il parere di cui all'articolo 49, in relazione alle sue competenze, nel caso in cui l'ente non abbia responsabili dei servizi;
e) roga, su richiesta dell'ente, i contratti nei quali l'ente è parte e autentica scritture private ed atti unilaterali nell'interesse dell'ente;
f) esercita ogni altra funzione attribuitagli dallo statuto o dai regolamenti, o conferitagli dal sindaco o dal presidente della provincia.

Al Segretario comunale può essere attribuita la Responsabilità di un'unità organizzativa, la gestione di budget assegnati con il PIAO / PEG o altro atto organizzativo ed il potere di emettere atti e provvedimenti di natura gestionale.

Il rapporto di lavoro dei segretari comunali e provinciali è disciplinato dai contratti collettivi nazionali e dalla contrattazione decentrata.

ART. 13 - VICE SEGRETARO COMUNALE

Il Comune di Pastrengo può dotarsi di un *Vice Segretario comunale*, anche con funzioni vicarie del Segretario comunale.

Il vice segretario svolge attività di collaborazione con il Segretario comunale e può adottare gli atti ad esso delegati dal Segretario comunale.

Sostituisce il Segretario comunale in caso di assenza o impedimento.

Le funzioni di vice segretario comunale possono essere svolte da un funzionario, in possesso dei requisii necessari per ricoprire il ruolo di segretario comunale.

ART. 14 - RESPONSABILE DI AREA

Il *Responsabile di Area* svolge, di norma, i seguenti compiti di seguito evidenziati:

a) pianifica, gestisce e coordina l'attività dell'area e del personale assegnato;
b) garantisce la corretta, funzionale ed efficiente erogazione dei servizi assegnati all'area;
c) gestisce e risolve tutti i problemi inerenti all'unità organizzativa comprese le eventuali sub-articolazioni;
d) gestisce i procedimenti amministrativi assegnati all'area con potere di delega;
e) garantisce la regolarità ammnistrativa delle procedure e dei provvedimenti di competenza dell'area;
f) esprime i pareri di regolarità tecnica sui provvedimenti di competenza dell'area;
g) propone proattivamente all'organo politico le azioni e gli interventi necessari per il funzionamento dell'area, degli eventuali uffici ad essa afferenti e dei servizi di competenza stimandone i costi;
h) realizza i programmi, persegue gli obiettivi e gestisce i fondi assegnati con il PIAO // DUP / PEG;
i) ricopre il ruolo di "preposto alla sicurezza" ai fini del d. lgs 81/2008;
j) esercita tutte le funzioni di cui all'art. 107 del d.lgs. 267/2000.

Il Ruolo di Responsabile d'area è classificato come posizione di responsabilità di direzione di unità organizzative di particolare complessità, caratterizzata da elevato grado di autonomia gestionale e organizzativa ed è automaticamente classificato come ruolo di Elevata Qualificazione (di tipo gestionale).

Il ruolo di Responsabile di area può essere attribuito a personale dipendente, anche acquisito dall'esterno con incarico a contratto, inquadrato nell'area dei funzionari e dell'EQ.

È riconosciuta la possibilità di attribuire l'incarico di Responsabile di area anche a personale in possesso di un contratto c.d di "scavalco di eccedenza"[9]

ART. 15 - RESPONSABILE DI UFFICIO

Il *Responsabile di Ufficio* riporta al Responsabile di area e svolge le seguenti funzioni:

a) garantisce la funzionalità dell'ufficio;
b) garantisce la correttezza dell'attività, delle procedure e degli atti emessi dall'ufficio;
c) gestisce e risolve tutti problemi inerenti l'ufficio;
d) coordina e gestisce il personale eventualmente assegnato all'ufficio;
e) fornisce al responsabile di area le informazioni necessarie per redigere i budget ed i report per il controllo di gestione;
f) ricopre la funzione di responsabile di procedimento (con potere di firma se assegnato dal responsabile di direzione) di tutti i procedimenti amministrativi assegnati all'unità organizzativa;
g) sostituisce il Responsabile di area o il Responsabile di un altro ufficio dell'area su delega o incarico del Responsabile di area in caso di assenza o impedimento di uno di questi [(10)].

Il ruolo di Responsabile di Ufficio può essere assegnato a personale inquadrato nell'area di funzionari / EQ o degli istruttori.

È riconosciuta la possibilità di attribuire l'incarico di Responsabile d'Ufficio anche a personale in possesso di un contratto c.d di "scavalco di eccedenza"[11]

ART. 16 - RESPONSABILE DI UNITÀ DI PROGETTO

[9] Così' Corte Conti Puglia n. 80/2022

[10] La scelta di affidare la sostituzione del Responsabile di area ad un dipendente assegnato alla stessa unità organizzativa è motivato dal fatto che un dipendente della stessa unità organizzativa conosce meglio le problematiche ed i procedimenti in corso rispetto ad altro responsabile di area.
Si ritiene che la sostituzione possa essere affidata anche ad un dipendente inquadrato in categoria C) dotato di adeguate competenze in forza della risposta CFL 140/bis in cui si riconosce la possibilità di affidare l'incarico di posizione organizzativa, in via temporanea ed eccezionale, ad un dipendente di categoria C anche in presenza di altre categorie D. la sostituzione può infatti essere inquadrato in un'ipotesi di esercizio di funzioni dirigenziali (funzionali) di carattere temporaneo ed eccezionale.

[11] Così' Corte Conti Puglia n. 80/2022

I compiti, poteri e le modalità di espletamento dell'incarico di *Responsabile di Unità di progetto* sono definiti nel provvedimento di costituzione dell'unità organizzativa temporanea e/o nel provvedimento di incarico.

Il ruolo di Responsabile di Unità di progetto può essere qualificato come ruolo di Elevata Qualificazione sia di tipo gestionale che di tipo specialistico, in base agli obiettivi assegnati all'Unità di progetto.

Il Ruolo di Responsabile di Unità di progetto può essere assegnato a personale inquadrato nell'area dei funzionari e EQ o dell'area degli istruttori.

È riconosciuta la possibilità di attribuire l'incarico di Responsabile di Unità di progetto anche a personale in possesso di un contratto c.d di "scavalco di eccedenza"[12]

ART. 17 - RESPONSABILE DI PROCEDIMENTO AMMINISTRATIVO

Responsabile di procedimento amministrativo è il dipendente incaricato dell'istruttoria del procedimento ed eventualmente del potere di emissione del provvedimento finale.

Il responsabile di procedimento è responsabile della corretta istruttoria del procedimento amministrativo, ed è responsabile della correttezza del provvedimento finale in caso di delega.[13]

Il ruolo di Responsabile di procedimento amministrativo può essere assegnato a personale inquadrato nell'area di funzionari / EQ o degli istruttori.

È riconosciuta la possibilità di attribuire l'incarico di Responsabile di Procedimento amministrativo anche a personale in possesso di un contratto c.d di "scavalco di eccedenza"[14]

ART. 18 - ASSISTENTE DI STRUTTURA

L'assistente di struttura supporta il responsabile dell'Unità organizzativa in cui è collocato e lo sostituisce in caso di assenza o impedimento.

È responsabile della corretta prestazione professionale connessa al ruolo ed al profilo.

---

[12] Così' Corte Conti Puglia n. 80/2022

[13] Il Responsible di procedimento è responsabile anche del provvedimento finale nel caso abbia ricevuto tale delega dal Responsabile di area

[14] Così' Corte Conti Puglia n. 80/2022

Può sostituire il Responsabile di area in caso di assenza o impedimento, operando sulla base delle indicazioni del Responsabile di area, il quale può indicare come sostituto anche altro responsabile area o il segretario comunale.

Il ruolo di assistente di struttura può essere ricoperto da profili professionali sia inquadrati nell'area dei funzionari / E.Q sia da profili professionali inquadrati nell'area degli istruttori, in base alle competenze e capacità del dipendente incaricato.

È riconosciuta la possibilità di attribuire l'incarico di Assistente di struttura anche a personale in possesso di un contratto c.d di "scavalco di eccedenza"[15]

ART. 19 - ADDETTO DI STRUTTURA

L'addetto di struttura è un ruolo organizzativo di tipo operativo e di supporto al Responsabile dell'Unità organizzativa in cui è collocato; può essere un ruolo di tipo amministrativo o tecnico.

L'addetto di struttura è responsabile della corretta prestazione professionale connessa al ruolo ed al profilo.

Il ruolo di addetto di struttura può essere attribuito a personale dell'area degli istruttori o degli operatori esperti (in base alle mansioni e/o prestazioni richieste al ruolo).

È riconosciuta la possibilità di attribuire l'incarico di Addetto di struttura anche a personale in possesso di un contratto c.d di "scavalco di eccedenza"[16]

ART. 20 - RESPONSABILE DELLA PREVENZIONE E DELLA CORRUZIONE

Il *Responsabile della prevenzione, della corruzione e della trasparenza*, d'ora in poi *RPCT,* è di norma il segretario comunale.

In mancanza del segretario comunale titolare o convenzionato (ad esempio in caso di segretario comunale a scavalco) l'incarico di RPCT può essere affidato ad altro funzionario appartenente all'area dei funzionari / EQ.

I compiti del RPCT sono stabiliti dall'articolo 1 Legge 6 novembre 2012, n. 190 *Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica*

[15] Così' Corte Conti Puglia n. 80/2022

[16] Così' Corte Conti Puglia n. 80/2022

amministrazione e dal Piano triennale della prevenzione della corruzione e/o dalla sezione prevenzione della corruzione del PIAO.

La nomina del RPCT è di competenza del Sindaco.

ART. 21 - DATORE DI LAVORO

Datore di lavoro ai sensi del d.lgs.81/2008 [17] nel comune di Pastrengo è il Sindaco [18]

Al datore di lavoro competono:

compiti non delegabili

a) la valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'articolo 28 del d.lgs. 81/2008 [19];

---

[17] **Art. 2 comma 1 lett. b) d.lgs. 81/2008**

Il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa. Nelle pubbliche amministrazioni invece è il dirigente al quale spettano i poteri di gestione, oppure il funzionario che pur non avendo qualifica dirigenziale ha autonomia gestionale dell'apparato che dirige

[18] Si ritiene di affidare l'incarico al Sindaco in quanto il Comune di Pastrengo è comune inferiore ai 5000 abitanti e quindi esiste la possibilità di affidare funzioni gestionali anche a rappresentanti degli organi politici ai sensi dell'articolo 53, comma 23, della l. n. 388/2000

[19] **Art. 28: Oggetto della valutazione dei rischi**

1. La valutazione di cui all'articolo 17, comma 1, lettera a), anche nella scelta delle attrezzature di lavoro e delle sostanze o delle ((miscele chimiche)) impiegate, nonché nella sistemazione dei luoghi di lavoro, deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, tra cui anche quelli collegati allo stress lavoro-correlato, secondo i contenuti dell'accordo europeo dell'8 ottobre 2004, e quelli riguardanti le lavoratrici in stato di gravidanza, secondo quanto previsto dal decreto legislativo 26 marzo 2001, n. 151, nonché quelli connessi alle differenze di genere, all'età, alla provenienza da altri Paesi e quelli connessi alla specifica tipologia contrattuale attraverso cui viene resa la prestazione di lavoro e i rischi derivanti dal possibile rinvenimento di ordigni bellici inesplosi nei cantieri temporanei o mobili, come definiti dall'articolo 89, comma 1, lettera a), del presente decreto, interessati da attività di scavo. (14) (28)

1-bis. La valutazione dello stress lavoro-correlato di cui al comma 1 è effettuata nel rispetto delle indicazioni di cui all'articolo 6, comma 8, lettera m-quater), e il relativo obbligo decorre dalla elaborazione delle predette indicazioni e comunque, anche in difetto di tale elaborazione, a fare data dal 1° agosto 2010.

2. Il documento di cui all'articolo 17, comma 1, lettera a), redatto a conclusione della valutazione, può essere tenuto, nel rispetto delle previsioni di cui all'articolo 53, su supporto informatico e deve essere munito anche tramite le procedure applicabili ai supporti informatici di cui all'articolo 53, di data certa o attestata dalla sottoscrizione del documento medesimo da parte del datore di lavoro, nonché, ai soli fini della prova della data, dalla sottoscrizione del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o del rappresentante dei lavoratori per la sicurezza territoriale e del medico competente, ove nominato, e contenere:

a) una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa. La scelta dei criteri di redazione del documento è rimessa al datore di lavoro, che vi provvede con criteri di semplicità, brevità e comprensibilità, in modo da garantirne la completezza e l'idoneità quale strumento operativo di pianificazione degli interventi aziendali e di prevenzione;

b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);

c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;

d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;

b) la designazione del responsabile del servizio di prevenzione e protezione dai rischi.

Spetta inoltre

Compiti delegabili

c) nominare il medico competente per l'effettuazione della sorveglianza sanitaria;

c) designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;

d) individuare il preposto o i preposti per l'effettuazione delle attività di vigilanza loro spettanti.

e) *affidare i compiti ai lavoratori e tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza*;

f) fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente;

g) prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;

h) richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;

---

f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

3. Il contenuto del documento di cui al comma 2 deve altresì rispettare le indicazioni previste dalle specifiche norme sulla valutazione dei rischi contenute nei successivi titoli del presente decreto.

3-bis. In caso di costituzione di nuova impresa, il datore di lavoro è tenuto ad effettuare immediatamente la valutazione dei rischi elaborando il relativo documento entro novanta giorni dalla data di inizio della propria attività. Anche in caso di costituzione di nuova impresa, il datore di lavoro deve comunque dare immediata evidenza, attraverso idonea documentazione, dell'adempimento degli obblighi di cui al comma 2, lettere b), c), d), e) e f), e al comma 3, e immediata comunicazione al rappresentante dei lavoratori per la sicurezza. A tale documentazione accede, su richiesta, il rappresentante dei lavoratori per la sicurezza. (9)

3-ter. Ai fini della valutazione di cui al comma 1, l'Inail, anche in collaborazione con le aziende sanitarie locali per il tramite del Coordinamento Tecnico delle Regioni e i soggetti di cui all'articolo 2, comma 1, lettera ee), rende disponibili al datore di lavoro strumenti tecnici e specialistici per la riduzione dei livelli di rischio. L'Inail e le aziende sanitarie locali svolgono la predetta attività con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

i) inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria e richiedere al medico competente l'osservanza degli obblighi previsti a suo carico nel presente decreto;

j) nei casi di sorveglianza sanitaria di cui all'articolo 41, comunicare tempestivamente al medico competente la cessazione del rapporto di lavoro;

k) adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

l) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

m) adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37;

n) astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;

o) consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;

p) consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a), anche su supporto informatico come previsto dall'articolo 53, comma 5, nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera r); il documento è consultato esclusivamente in azienda

q) elaborare il documento di cui all'articolo 26, comma 3 anche su supporto informatico come previsto dall'articolo 53, comma 5, e, su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza. Il documento è consultato esclusivamente in azienda;

r) prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;

s) comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, entro 48 ore dalla ricezione del certificato medico, a fini statistici e informativi, i dati e le informazioni relativi agli infortuni sul lavoro che comportino l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni; l'obbligo di comunicazione degli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni si considera comunque assolto per mezzo della denuncia di cui all'articolo 53 del testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali, di cui al decreto del Presidente della Repubblica 30 giugno 1965, n. 1124;

t) consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50 del d. lgs 81/2008[20];

---

[20] **Art. 50 d. lgs 81/2008: Attribuzioni del rappresentante dei lavoratori per la sicurezza**

1. Fatto salvo quanto stabilito in sede di contrattazione collettiva, il rappresentante dei lavoratori per la sicurezza:
a) accede ai luoghi di lavoro in cui si svolgono le lavorazioni;
b) è consultato preventivamente e tempestivamente in ordine alla valutazione dei rischi, alla individuazione, programmazione, realizzazione e verifica della prevenzione nella azienda o unità produttiva;
c) è consultato sulla designazione del responsabile e degli addetti al servizio di prevenzione, alla attività di prevenzione incendi, al primo soccorso, alla evacuazione dei luoghi di lavoro e del medico competente;
d) è consultato in merito all'organizzazione della formazione di cui all'articolo 37;
e) riceve le informazioni e la documentazione aziendale inerente alla valutazione dei rischi e le misure di prevenzione relative, nonché quelle inerenti alle sostanze ed ai
((miscele pericolose))
, alle macchine, agli impianti, alla organizzazione e agli ambienti di lavoro, agli infortuni ed alle malattie professionali;
f) riceve le informazioni provenienti dai servizi di vigilanza;
g) riceve una formazione adeguata e, comunque, non inferiore a quella prevista dall'articolo 37;
h) promuove l'elaborazione, l'individuazione e l'attuazione delle misure di prevenzione idonee a tutelare la salute e l'integrità fisica dei lavoratori;
i) formula osservazioni in occasione di visite e verifiche effettuate dalle autorità competenti, dalle quali è, di norma, sentito;
l) partecipa alla riunione periodica di cui all'articolo 35;
m) fa proposte in merito alla attività di prevenzione;
n) avverte il responsabile della azienda dei rischi individuati nel corso della sua attività;
o) può fare ricorso alle autorità competenti qualora ritenga che le misure di prevenzione e protezione dai rischi adottate dal datore di lavoro o dai dirigenti e i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro.
2. Il rappresentante dei lavoratori per la sicurezza deve disporre del tempo necessario allo svolgimento dell'incarico senza perdita di retribuzione, nonché dei mezzi e degli spazi necessari per l'esercizio delle funzioni e delle facoltà riconosciutegli, anche tramite l'accesso ai dati, di cui all'articolo 18, comma 1, lettera r), contenuti in applicazioni informatiche. Non può subire

u) adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;

v) nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro;

w) nelle unità produttive con più di 15 lavoratori, convocare la riunione periodica di cui all'articolo 35;

x) aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

y) comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, in caso di nuova elezione o designazione, i nominativi dei rappresentanti dei lavoratori per la sicurezza; in fase di prima applicazione l'obbligo di cui alla presente lettera riguarda i nominativi dei rappresentanti dei lavoratori già eletti o designati;

z) vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità.

---

pregiudizio alcuno a causa dello svolgimento della propria attività e nei suoi confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.
3. Le modalità per l'esercizio delle funzioni di cui al comma 1 sono stabilite in sede di contrattazione collettiva nazionale.
4. Il rappresentante dei lavoratori per la sicurezza, su sua richiesta e per l'espletamento della sua funzione, riceve copia del documento di cui all'articolo 17, comma 1, lettera a).
5. I rappresentanti dei lavoratori per la sicurezza dei lavoratori rispettivamente del datore di lavoro committente e delle imprese appaltatrici, su loro richiesta e per l'espletamento della loro funzione, ricevono copia del documento di valutazione dei rischi di cui all'articolo 26, comma 3.
6. Il rappresentante dei lavoratori per la sicurezza è tenuto al rispetto delle disposizioni di cui al decreto legislativo 30 giugno 2003, n. 196 e del segreto industriale relativamente alle informazioni contenute nel documento di valutazione dei rischi e nel documento di valutazione dei rischi di cui all'articolo 26, comma 3, nonché al segreto in ordine ai processi lavorativi di cui vengono a conoscenza nell'esercizio delle funzioni.
7. L'esercizio delle funzioni di rappresentante dei lavoratori per la sicurezza è incompatibile con la nomina di responsabile o addetto al servizio di prevenzione e protezione.

Il Sindaco, in qualità di datore di lavoro, con proprio atto, può delegare tutte le funzioni di cui al comma precedente ad eccezione delle funzioni di cui alle lettere a) e b) che, per legge [21], non sono delegabili.

ART. 22 - PREPOSTO ALLA SICUREZZA

Il ruolo di *Preposto alla sicurezza* è ricoperto, di norma, dai diversi Responsabili di Area, per le attività e funzioni attribuite all'unità organizzativa da essi diretta.

Al Preposto competono i seguenti compiti:

a) sovrintendere e vigilare sull'osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di rilevazione di comportamenti non conformi alle disposizioni e istruzioni impartite dal datore di lavoro e dai dirigenti ai fini della protezione collettiva e individuale, intervenire per modificare il comportamento non conforme fornendo le necessarie indicazioni di sicurezza. In caso di mancata attuazione delle disposizioni impartite o di persistenza dell'inosservanza, interrompere l'attività del lavoratore e informare i superiori diretti))

b) verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;

c) richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

d) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

e) astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;

---

21 **Art. 17 d. lgs. 81/2008**

f) segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;

g) in caso di rilevazione di deficienze dei mezzi e delle attrezzature di lavoro e di ogni condizione di pericolo rilevata durante la vigilanza, se necessario, interrompere temporaneamente l'attività e, comunque, segnalare tempestivamente al datore di lavoro e al dirigente le non conformità rilevate))

I preposti esercitano inoltre tutti i compiti delegati con apposito atto dal datore di lavoro.

ART. 23 - RESPONSABILE SERVIZIO PREVENZIONE E PROTEZIONE

Il servizio di prevenzione e protezione è composto dal Responsabile del servizio di prevenzione e protezione e dai Preposti alla sicurezza.

Il Responsabile del servizio di prevenzione e protezione, d'ora in poi RSPP, è di norma un soggetto esterno con adeguate competenze in materia.

Il datore di lavoro definisce i compiti del RSPP con l'atto di nomina o con atto integrativo successivo.

ART. 24 - RESPONSABILE ANTICENDI

Il *Responsabile delle attività in materia di prevenzione incendi* del Comune di Pastrengo, ai sensi e per gli effetti della normativa vigente, è individuato nel Responsabile dell'Area Tecnica.

ART 25 - RESPONSABILE DELLA GESTIONE DOCUMENTALE

Il *Responsabile della gestione documentale* è il funzionario cui compete la gestione del *Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi* di cui all'articolo 61 del d. lgs 445/2000.[22]

[22] **Art. 61 Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi**
1. Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50. Il servizio è posto alle dirette dipendenze della stessa area organizzativa omogenea.

Al Responsabile della gestione documentale spetta, di norma, il compito di elaborare il manuale di gestione documentale [23], nonché:

a) attribuire il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del presente testo unico
c) garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;
d) curare che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;

---

2. Al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.
3. Il servizio svolge i seguenti compiti:
a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del presente testo unico;
c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53;
d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
e) conserva le copie di cui agli articoli 62 e 63, in luoghi sicuri differenti;
f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
g) autorizza le operazioni di annullamento di cui all'articolo 54;
h) vigila sull'osservanza delle disposizioni del presente testo unico da parte del personale autorizzato e degli incaricati.

[23] **Il manuale di gestione documentale riguarda**: la formazione, gestione, trasmissione, interscambio, accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione; Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle: ○ misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti; ○ delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta; ○ indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID (rif. linee guida AGID 2021)

e) conservare le copie di cui agli articoli 62 [(24)] e 63 [(25)] del dPR 445/2000, in luoghi sicuri differenti;

f) garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi

[24] **Art. 62 (R) Procedure di salvataggio e conservazione delle informazioni del sistema**

1. Il responsabile per la tenuta del sistema di gestione informatica dei documenti dispone per la corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile.
2. E' consentito il trasferimento su supporto informatico rimovibile delle informazioni di protocollo relative ai fascicoli che fanno riferimento a procedimenti conclusi.
3. Le informazioni trasferite sono sempre consultabili. A tal fine, il responsabile per la tenuta del sistema di gestione informatica dei documenti dispone, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale, la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici.
4. Le informazioni relative alla gestione informatica dei documenti costituiscono parte integrante del sistema di indicizzazione e di organizzazione dei documenti che sono oggetto delle procedure di conservazione sostitutiva.

[25] **Art. 63 (R) Registro di emergenza**

1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. (R)
2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. (R)
3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. (R)
4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. (R)
5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza. (R)

documentali, incluse le funzionalità di accesso di cui agli articoli 59[26] e 60[27] e le attività di gestione degli archivi di cui agli articoli 67[28], 68[29] e 69[30];

g) autorizzare le operazioni di annullamento di cui all'articolo 54 del dPr 445/2000 [31];

---

[26] **Art. 59 (R) Accesso esterno**

1. Per l'esercizio del diritto di accesso ai documenti amministrativi, possono essere utilizzate tutte le informazioni del sistema di gestione informatica dei documenti anche mediante l'impiego di procedure applicative operanti al di fuori del sistema e strumenti che consentono l'acquisizione diretta delle informazioni da parte dell'interessato.
2. A tal fine le pubbliche amministrazioni determinano, nel rispetto delle disposizioni di legge sulla tutela della riservatezza dei dati personali, e nell'ambito delle misure organizzative volte ad assicurare il diritto di accesso ai documenti amministrativi i criteri tecnici ed organizzativi per l'impiego, anche per via telematica, del sistema di gestione informatica dei documenti per il reperimento, la visualizzazione e la stampa delle informazioni e dei documenti.
3. Nel caso di accesso effettuato mediante strumenti che consentono l'acquisizione diretta delle informazioni e dei documenti da parte dell'interessato, le misure organizzative e le norme tecniche indicate al comma 2 determinano, altresì, le modalità di identificazione del soggetto anche mediante l'impiego di strumenti informatici per la firma digitale del documento informatico, come disciplinati dal presente testo unico.
4. Nel caso di accesso effettuato da soggetti non appartenenti alla pubblica amministrazione possono utilizzarsi le funzioni di ricerca e di visualizzazione delle informazioni e dei documenti messe a disposizione – anche per via telematica – attraverso gli uffici relazioni col pubblico**.**

[27] **Art. 60 (R) Accesso effettuato dalle pubbliche amministrazioni**

1. Le pubbliche amministrazioni che, mediante proprie applicazioni informatiche, accedono al sistema di gestione informatica dei documenti delle grandi aree organizzative omogenee di cui al comma 4 dell'articolo 50, adottano le modalità di interconnessione stabilite nell'ambito delle norme e dei criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni.
2. Le pubbliche amministrazioni che accedono ai sistemi di gestione informatica dei documenti attraverso la rete unitaria delle pubbliche amministrazioni utilizzano funzioni minime e comuni di accesso per ottenere le seguenti informazioni:
   a) numero e data di registrazione di protocollo dei documenti, ottenuti attraverso l'indicazione alternativa o congiunta dell'oggetto, della data di spedizione, del mittente, del destinatario;
   b) numero e data di registrazione di protocollo del documento ricevuto, ottenuti attraverso l'indicazione della data e del numero di protocollo attribuiti dall'amministrazione al documento spedito.
3. Ai fini del presente articolo, le pubbliche amministrazioni provvedono autonomamente, sulla base delle indicazioni fornite dall'Autorità per l'informatica nella pubblica amministrazione, alla determinazione dei criteri tecnici ed organizzativi per l'accesso ai documenti e alle informazioni del sistema di gestione informatica dei documenti.

[28] **Art. 67 (R) Trasferimento dei documenti all'archivio di deposito**

1. Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione. (R)
2. Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente. (R)
3. Il responsabile del servizio per la gestione dei flussi documentali e degli archivi deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito. (

[29] **Art. 68 (R) Disposizioni per la conservazione degli archivi**

1. Il servizio per la gestione dei flussi documentali e degli archivi elabora ed aggiorna il piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni contenute in materia di tutela dei beni culturali e successive modificazioni ed integrazioni.
2. Dei documenti prelevati dagli archivi deve essere tenuta traccia del movimento effettuato e della richiesta di prelevamento.
3. Si applicano in ogni caso, per l'archiviazione e la custodia dei documenti contenenti dati personali, le disposizioni di legge sulla tutela della riservatezza dei dati personali**.**

[30] **Art. 69 (R) Archivi storici**

1. I documenti selezionati per la conservazione permanente sono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso, negli Archivi di Stato competenti per territorio o nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

[31] **Art. 54 (R) Informazioni annullate o modificate**

1. Le informazioni non modificabili di cui all'articolo 53 lett. a), b), c), d), e) e f) sono annullabili con la procedura di cui al presente articolo. Le informazioni annullate devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura.

h) vigila sull'osservanza delle disposizioni normative in materia da parte del personale autorizzato e degli incaricati.

Il ruolo di Responsabile della gestione documentale è affidato ad un dipendente inquadrato nell'area dei funzionari e dell'EQ , al Sindaco o al Segretario comunale.

ART. 26 - RESPONSABILE DELLA CONSERVAZIONE

Il *Responsabile della conservazione* opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD.[32]

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

In particolare, il Responsabile della conservazione:

a) definisce le politiche di conservazione ed i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

---

2. La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione.

32 **Art. 44 CAD comma 1 quater: 1-quater**. Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis.

c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede a versare i documenti;

Il Responsabile della conservazione può affidare ad un soggetto esterno, denominabile "Conservatore", l'incarico della conservazione digitale dei documenti.
La gestione della conservazione dei documenti è regolata dal "manuale di conservazione".
Il ruolo di Responsabile della conservazione può essere affidato ad un dipendente inquadrato nell'area dei funzionari e dell'EQ oppure dell'area degli istruttori.

ART. 27 - RESPONSABILE TRANSIZIONE DIGITALE

Al Responsabile della Transizione Digitale, d'ora in poi RTD sono attribuiti i seguenti compiti:

a) pianificare e coordinare lo sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
b) indirizzare e coordinare lo sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c) indirizzare, pianificare, coordinare e monitorare la sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 del d.lgs. 82/2005 (dpcm 13.11.2014) ;
d) garantire l'accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
e) analizzare periodicamente la coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
f) cooperare alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
g) indirizzare, coordinare e monitorare la pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) progettare e coordinare le iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a soggetti giuridici mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i) promuovere le iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
j) pianificare e coordinare il processo di diffusione, all'interno dell'amministrazione, dei

sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis del d.lgs 82/2005;

k) pianificare e coordinare gli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b), ed eventualmente gestire i budget assegnati;
l) proporre il piano triennale degli acquisti informatici sulla base delle indicazioni fornite da AGID alle amministrazioni pubbliche;
m) proporre ed eventualmente gestire i budget assegnati per mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati personali sia effettuato conformemente al GDPR, alla normativa nazionale, alle regole deontologiche allegate al Codice Privacy ed alle linee guida del Garante;
n) nominare gli amministratori di sistema definendone compiti, funzioni e responsabilità o attribuendo gli incarichi all'esterno con apposito contratto di servizio;
o) tenere l'elenco degli amministratori di sistema anche esterni;
p) controllare e supervisionare l'attività degli altri amministratori di sistema, soprattutto esterni, valutandola anche attraverso l'esame della relazione annuale predisposta dagli stessi;
q) costituire tavoli di coordinamento con le altre posizioni apicali ed emettere circolari negli ambiti di propria competenza (digitalizzazione ed eventualmente privacy e protezione dei dati).

Il ruolo di RTD può essere affidato ad un dipendente inquadrato nell'area dei funzionari e dell'EQ o al Sindaco o al Segretario comunale.

ART. 28 - TITOLARE TRATTAMENTO DATI PERSONALI

Titolare del trattamento dati, ai sensi dell'art. 4 paragrafo 1 punto 7) del Regolamento**,** è *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.

Titolare del trattamento dei dati personali è il Comune di Pastrengo ed il Sindaco, che in base all'articolo 50 comma 2 del d.lgs. 267/2000 ha la legale rappresentanza dell'ente, esercita le funzioni di Titolare del trattamento dei dati personali.

Pertanto, al sindaco, nella qualità di soggetto che esercita le funzioni di titolare di trattamento dei dati personali sono attribuiti i seguenti compiti/poteri:

a) definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici nel DUP e negli altri documenti di programmazione e pianificazione del Comune;
b) mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Codice Privacy (d.lgs. 1996/2003 e smi) ed al GDPR;
c) delegare, con proprio atto, i dirigenti / titolari di posizione organizzativa a svolgere i compiti, le funzioni e i poteri in ordine ai processi, procedimenti e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste 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, all'eventuale uso di apparecchiature di videosorveglianza;
d) formare e aggiornare l'elenco dei Dirigenti / Posizioni Organizzative, delegati e preposti al trattamento dei dati ed eventualmente pubblicarlo sul sito web istituzionale dell'ente titolare;
e) nominare il Referente / Coordinatore Privacy;
f) designare, con proprio atto, il Responsabile per la protezione dei dati personali (DPO) o fornire linee di indirizzo per l'affidamento del servizio all'esterno;
g) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
h) favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi

di categoria rappresentativi;

i) favorire l'adesione a meccanismi di certificazione;

j) assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

Il Sindaco potrà delegare, in tutto o in parte, i poteri (ed i doveri) di Titolare del trattamento Responsabili di area in qualità di "*Preposti al trattamento dei dati*", o al dipendente eventualmente nominato referente / coordinatore privacy.

ART. 29 - CONTITOLARE DI TRATTAMENTO

La contitolarità [33] si verifica allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del Regolamento UE 679/2016. [34]

L'accordo può individuare un punto di contatto per gli interessati e deve riflettere adeguatamente i rispettivi ruoli e rapporti dei contitolari con gli interessati.

Il contenuto essenziale dell'accordo è messo a disposizione degli interessati attraverso la pubblicazione su apposita sezione del sito web dell'ente.

Indipendentemente dalle disposizioni dell'accordo l'interessato potrà comunque esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

ART. 30 - RESPONSABILE DI TRATTAMENTO

I *Responsabile (esterno) di trattamento* [35], è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

---

33 Art. 26 regolamento UE 679/2016

34 Si tratta delle informative privacy da rendere prima dell'inizio del trattamento dati personali

35 Articolo 4 par. 1 punto 8) del Regolamento UE 679/2016

Il Titolare del trattamento, o suo delegato, può affidare a soggetti terzi il trattamento dei dati per suo conto (si pensi all'esternalizzazione di servizi che comportano il trattamento dei dati).

Per garantire che siano rispettate le prescrizioni del Regolamento il Titolare può affidare le attività di trattamento solo a Responsabili che presentino garanzie sufficienti, in termini di conoscenza specialistica, affidabilità e risorse, e che mettano in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento.

L'esecuzione dei trattamenti da parte di un Responsabile del trattamento deve essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il Responsabile del trattamento al Titolare del trattamento.

Contenuto dell'accordo

L'accordo, ai sensi dell'articolo 28 del Regolamento UE 679/2016, deve contenere:

a) materia disciplinata;
b) durata del trattamento;
c) la natura e la finalità del trattamento;
d) il tipo di dati personali;
e) le categorie di interessati;
f) gli obblighi e i diritti del titolare del trattamento.

L'accordo deve prevedere che il Responsabile del trattamento:

(i) tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento;
(ii) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
(iii) adotti tutte le misure richieste dall'articolo 32 del RGPD (misure di sicurezza) [(36)];

36 **Art. 32: Sicurezza del trattamento (C83**) 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi,

(iv) ricorra ad altro responsabile del trattamento solo su consenso del Titolare del trattamento e stipuli con il sub responsabile un accordo che abbia gli stessi contenuti dell'accordo fra Titolare e Responsabile principale;

(v) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del RGPD;

(vi) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD [(37)], tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

---

conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

37 **Art. 33: Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)** 1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. 3. La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; 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 titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. 4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. 5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 Comunicazione di una violazione dei dati personali all'interessato (C86-C88) 1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. 2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). 3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano 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 titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. 4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta

Articolo 35 Valutazione d'impatto sulla protezione dei dati (C84, C89-C93, C95) 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. 2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno. 3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato,

(vii) su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

---

compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. 4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68. 5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato. 6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. 7. La valutazione contiene almeno: 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 proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. 8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati. 9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti. 10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento. 11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Art. 36 Consultazione preventiva (C94-C96) 1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. 2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione. 3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale; b) le finalità e i mezzi del trattamento previsto; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; d) ove applicabile, i dati di contatto del responsabile della protezione dei dati; e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; e f) ogni altra informazione richiesta dall'autorità di controllo. 4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento. 5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

(viii) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del RGPD, consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;

(ix) informi immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

ART. 31 - RESPONSABILE PROTEZIONE DATI

Il *Responsabile Protezione Dati*, d'ora in poi RPD o DPO (*Data Protection Officier*) può essere un soggetto interno o un soggetto esterno incaricato della copertura del ruolo con contratto di prestazione di servizi.

In caso di affidamento dell'incarico ad un soggetto interno questo avviene con provvedimento del sindaco; in caso di affidamento all'esterno questo è affidato dal RTD sulla base delle eventuali linee di indirizzo fornite dagli Organi di Governo (Giunta Comunale o Sindaco).

Al DPO (*Data Protection Officier*) sono attribuiti i seguenti compiti:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento dei dati, tra cui la consultazione

preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

Al DPO possono essere assegnati anche altri compiti, oltre a quelli sopra indicati, sempre che non determinino incompatibilità o conflitto di interesse.

Il rapporto fra Ente e DPO va regolato da un contratto di prestazione di servizi.

Il DPO riporta al Sindaco in qualità di soggetto che esercita le funzioni di Titolare di trattamento o a soggetto da questi delegato.

ART. 32 - REFERENTE // COORDINATORE PRIVACY

Il ruolo di *Coordinatore/Referente privacy*, è attribuito dal sindaco, di norma al RTD o ad altro funzionario, e con l'atto di nomina possono essere attribuiti i seguenti compiti:

a) proporre gli obiettivi strategici ed operativi per il costante adeguamento dell'organizzazione ai dettati del GDPR, alla normativa nazionale, alle regole deontologiche collegate al Codice Privacy ed alle linee guida del Garante, proponendo l'inserimento di tali obiettivi strategici e/o operativi nel DUP // PIAO e negli altri documenti di programmazione e pianificazione del titolare;
b) proporre ed eventualmente gestire il budget assegnato per mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al GDPR, alla normativa nazionale, alle regole deontologiche allegate al Codice Privacy ed alle linee guida del Garante;
c) coordinare l'attività dei dirigenti/titolari di posizione organizzativa nello svolgimento delle funzioni e dei compiti in ordine ai processi, procedimenti e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, fornendo ad essi le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste 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, all'eventuale uso di apparecchiature di videosorveglianza;
d) formare e aggiornare l'elenco dei *Preposti* al trattamento dei dati delegati dal Titolare ed eventualmente pubblicarlo sul sito web istituzionale del titolare;

e) gestire il procedimento di affidamento all'esterno del ruolo di DPO sulla base degli indirizzi stabiliti dagli organi politici;
f) effettuare, anche in collaborazione con il DPO nominato, periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati ed alla formazione dei dipendenti;
g) gestire, eventualmente con il supporto del DPO, il processo di Valutazione d'impatto (DPIA);
h) favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
i) favorire l'adesione a meccanismi di certificazione;
j) gestire, unitamente al DPO, i contatti con gli interessati che intendono esercitare i diritti garantiti dal GDPR.
k) Gestire, unitamente al DPO, i contatti con il Garante privacy.

L'incarico è affidato, di norma, ad un dipendente inquadrato nell'area dei funzionari o dell'EQ.

ART. 33 - PREPOSTI AL TRATTAMENTO DEI DATI

I Responsabili di Area sono, di norma, nominati *Preposti al trattamento dei dati;* ad essi potrà quindi essere attribuita un'ampia delega volta:

- al compimento di tutte le attività necessarie, utili o anche solo opportune per individuare e nominare i responsabili del trattamento di cui all'art. 28 del Regolamento (UE) 2016/679, definiti come quei soggetti, persone fisiche o giuridiche, che trattano dati personali per conto del titolare del trattamento, in nome e per conto dell'Ente.
- al compimento di tutte le attività necessarie, utili o anche solo opportune per individuare e nominare i soggetti addetti e/o autorizzati al trattamento, in nome e per conto dell'Ente.
- a sottoscrivere, anche con firma digitale, tutti gli atti, le dichiarazioni, i contratti necessari tra l'Ente, l'Amministrazione e/o soggetti terzi e, in generale, a compiere tutte le attività necessarie, utili o anche solo opportune, alla corretta esecuzione delle funzioni proprie dell'Ente in qualità di titolare del trattamento

In particolare, potranno essere loro attribuite le seguenti funzioni:

a) trattare i dati personali su istruzione del titolare del trattamento;
b) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) garantire il tempestivo ed integrale rispetto dei doveri del titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR[38];
d) osservare le disposizioni contenute negli atti generali di organizzazione dell'ente nonché le specifiche istruzioni impartite dal titolare;
e) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute negli atti generali di organizzazione adottati dall'ente, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
f) collaborare con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con il Referente privacy, l'Amministratore di sistema e con le altre strutture competenti individuate dal

---

38 **Articolo 32**: **Sicurezza del trattamento**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Titolare;[39]

g) curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del Titolare per l'applicazione del Codice, del GDPR, e degli altri atti di natura generale;
h) assistere il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
i) assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
j) mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, GDPR e nel presente Regolamento;
k) contribuire alle attività di verifica del rispetto del Codice e del GDPR, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato;
l) curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza: (i) elenco dei contitolari, dei responsabili dei trattamenti, e degli addetti al trattamento, con i relativi punti di contatto; (ii) elenco degli archivi/ banche dati;
m) garantire l'aggiornamento, almeno annuale, della ricognizione dei trattamenti di competenza;
n) fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/DPO) nell'esercizio delle sue funzioni.

[39] Il coinvolgimento del DPO è possibile ma eventuale. Dipende da come viene strutturato il sistema organizzativo privacy e dal contratto di incarico del DPO.

Ogni Preposto, nell'espletamento dei propri compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, sarà obbligato a:

i) comunicare tempestivamente a chi gestisce il registro dei trattamenti, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;

ii) collaborare con il titolare nella redazione della valutazione d'impatto sulla protezione dei dati[40] e nella consultazione preventiva [41];

iii) predisporre le informative previste e verificarne il rispetto;

iv) fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;

v) designare gli addetti e autorizzati al trattamento, e fornire loro specifiche istruzioni;

vi) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;

vii) garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa del titolare ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;

viii) informare il titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Ciascun Preposto risponde al Titolare del trattamento di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.

Il preposto al trattamento collabora con il referente privacy e con il DPO.

ART. 34 -ADDETTO AL TRATTAMENTO DEI DATI

[40] Valutazione d'impatto o DPIA è prevista dall'art. 35 del Regolamento.

[41] La consultazione preventiva del Garante è prevista dall'articolo 36 del Regolamento e si attiva quando dalla DPIA effettuata a norma dell'articolo 35 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

Per “Addetto al trattamento dei dati personali” si devono intendere quindi tutti quei soggetti che effettuano materialmente le operazioni di trattamento sui dati personali [42].

L’Addetto al trattamento dei dati personali è, di norma, un soggetto interno all’ente che opera in base alle istruzioni ed indicazioni impartite dal Titolare per il tramite degli organi di indirizzo dell’ente o dei soggetti designati come Preposti.

L’incarico di “Addetto” al trattamento dei dati avviene con atto del Preposto (Responsabile di Area).

ART. 35 - AMMINISTRATORI DI SISTEMA

Per "Amministratore di sistema" si devono intendere quelle figure professionali (interne o esterne all’azienda) che hanno il compito di provvedere alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti.

Gli Amministratori di sistema, a titolo esemplificativo, possono essere così classificati

- *Amministratori di dominio:* si tratta degli Amministratori dei domini Active Directory interni ed esterni; rientrano in questa categoria i componenti dei gruppi “Domain Admins” e tutti coloro che, attraverso un meccanismo di delega, hanno la possibilità di agire su un sottoinsieme degli oggetti dei domini;
- *Amministratori di server*: si tratta degli utenti che hanno diritti amministrativi su uno o più server; rientrano in questa categoria, a titolo esemplificativo, gli utenti appartenenti al gruppo “Administrators” di uno o più server Windows o gli utenti di uno o più server Linux che, attraverso il comando “sudo”, possono impersonare l’utente “root”;
- *Amministratori di basi di dati:* rientrano in questa categoria gli utenti che hanno la possibilità di manipolare la struttura di uno o più database attraverso comandi di “Data Definition Language”;
- *Amministratori di apparati di rete*: rientrano in questa categoria gli utenti che hanno la possibilità di accedere ad apparati di rete layer 2 o layer 3 e modificarne le configurazioni;

[42] Si tratta (di fatto) degli (ex) “incaricati al trattamento previsti dall’articolo 30 del codice privacy ora abrogato.

- *Amministratori di apparati di sicurezza*: rientrano in questa categoria gli utenti che possono modificare le configurazioni di sistemi hardware o software dedicati alla sicurezza, quali ad esempio firewall, sistemi di intrusion prevention, web proxy e sistemi antivirus
- *Amministratori di software complessi:* rientrano in questa categoria gli utenti che possono agire sui software in uso (ad esempio il gestionale, il software per la fatturazione ecc.) ma che non hanno acceso a credenziali amministrative del server su cui operano
- *Amministratori dei sistemi di Backup:* rientrano in questa categoria gli utenti che gestiscono ed implementano le operazioni di backup e che sovrintendono al loro corretto funzionamento

Il Garante privacy nel provvedimento 27 novembre 2008" doc web n. 1577499 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*, ancora applicabile perché coerente con il Regolamento UR 679/2016, fornisce le seguenti indicazioni in ordine agli amministratori di sistema:

- *valutazione caratteristiche soggettive*: l´attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell´esperienza, della capacità e dell´affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- *designazioni individuali*: la designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l´elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- *elenco amministratori di sistema*: gli estremi identificativi delle persone fisiche amministratori di sistema, con l´elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante e qualora l´attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di

lavoratori, i titolari di trattamento pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l´identità degli amministratori di sistema nell´ambito delle proprie organizzazioni, secondo le caratteristiche dell´azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti, ciò, avvalendosi dell´informativa resa agli interessati ai sensi dell´art. 13 del Codice (ndr: ora Regolamento) nell´ambito del rapporto di lavoro che li lega al titolare, oppure tramite un disciplinare tecnico;

- *verifica delle attività*: l´operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un´attività di verifica da parte dei Titolari o dei Responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- *registrazione degli accessi*: devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell´evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi
- *servizi in outsourcing*: nel caso di servizi di amministrazione di sistema affidati in outsourcing il Titolare o il Responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali "Amministratori di sistema". Il contratto di affidamento del servizio all'esterno deve necessariamente prevedere fra le clausole contrattuali la registrazione e messa a disposizione degli access log. L'amministratore di sistema esterno deve elaborare almeno annualmente una relazione sull'attività. La relazione e l'attività svolta è sottoposta a controllo da parte del titolare.

All'Amministratore di sistema, spettano di norma i seguenti compiti:

a) Gestire il sistema informativo-informatico inteso come complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni personali, attenendosi anche alle disposizioni del Titolare in tema di sicurezza;

b) Predisporre ed aggiornare un sistema di sicurezza informatico tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, misure che comprendono, tra le altre, se del caso:
   (i) la pseudomizzazione e la cifratura dei dati personali;
   (ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   (iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   (iv) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

c) Collaborare nella predisposizione del Piano protezione dati per la parte concernente il sistema informatico ed il trattamento informatico dei dati; [43]

d) Elaborare e tenere aggiornato un disciplinare tecnico da portare in approvazione al Titolare del trattamento in cui siano disciplinati le misure e le procedure di sicurezza aziendali in tema di gestione del sistema informativo-informatico;

e) Elaborare e tenere aggiornato un disciplinare tecnico per la gestione della posta elettronica ed internet;

f) Elaborare e tenere aggiornato un sistema di valutazione dei rischi;

g) Cooperare nella predisposizione della Valutazione d'impatto sulla protezione dati ai sensi dell'articolo 35 del Regolamento (anche DPIA – data protection impact assessement);

---

43 I dati particolari (ex sensibili) devono essere soggetti a forme rafforzate di sicurezza (gestione separata).

h) Collaborare con il titolare e gli altri ruoli dell'organigramma privacy in caso di data breach;
i) Redigere una relazione annuale sull'attività svolta in modo da permetterne la verifica;
j) Vigilare sugli interventi informatici effettuati sul sistema informativo-informatico dell'ente e sull'impianto di videosorveglianza effettuati da vari operatori esterni ed in caso di anomalie segnalarle al RTD, Referente / Coordinatore privacy ed al Responsabile Protezione Dati / DPO (Data protection officier);
k) Coordinare assieme al Titolare, al Responsabile della Transizione Digitale, al Responsabile della Protezione Dati ed al Referente privacy le attività operative degli addetti ai trattamenti informatici nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico.
l) Collaborare con il Titolare ed il DPO per l'attuazione delle prescrizioni impartite dal Garante;
m) Comunicare prontamente al Titolare qualsiasi situazione di cui sia venuto a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;
n) Verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore installati nei pc. presenti nell'unità produttiva;
o) Adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (*log in e log out*) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
p) assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Disciplinare tecnico, e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli incaricati del trattamento dati, svolgendo anche la funzione di custode delle copie delle credenziali;

q) procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;

r) adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche in conformità allo stesso Disciplinare tecnico;

s) adottare tutti i provvedimenti e le azioni necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico (*disaster recovery*) degli stessi con copie di *back-up*, vigilando sulle procedure attivate in struttura. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;

t) indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;

u) Compiere tutte le attività necessarie, utili o anche solo opportune per garantire l'adeguata sicurezza del sistema informativo-informatico;

v) Autorizzare altri dipendenti al trattamento dei dati connessi al sistema informatico in qualità di "addetti al trattamento dei connessi al sistema informativo-informatico" definendo compiti, poteri ed ambiti di autorizzazione.

w) Proporre al Responsabile della Transizione Digitale gli investimenti per l'implementazione del sistema di sicurezza informatica.

Gli amministratori di sistema sono individuati dal RTD. In caso di assenza di profili professionali adeguati all'interno, il RTD l'incarico può essere affidato ad un soggetto esterno con apposito contratto di servizio.

ART. 36 - ORGANO DI REVISIONE ECONOMICO – FINANZIARIA

L'Organo di Revisione economico-finanziaria del Comune di Pastrengo è composto da un unico revisore, nominato dal Consiglio comunale.

L'organo di revisione svolge le seguenti funzioni:

a) attività di collaborazione con l'organo consiliare secondo le disposizioni dello statuto e del regolamento;
b) pareri, con le modalità stabilite dal regolamento, in materia di:
    i) strumenti di programmazione economico-finanziaria;
    ii) proposta di bilancio di previsione verifica degli equilibri e variazioni di bilancio escluse quelle attribuite alla competenza della giunta, del responsabile finanziario e dei dirigenti, a meno che il parere dei revisori sia espressamente previsto dalle norme o dai principi contabili, fermo restando la necessità dell'organo di revisione di verificare, in sede di esame del rendiconto della gestione, dandone conto nella propria relazione, l'esistenza dei presupposti che hanno dato luogo alle variazioni di bilancio approvate nel corso dell'esercizio, comprese quelle approvate nel corso dell'esercizio provvisorio;
    iii) modalità di gestione dei servizi e proposte di costituzione o di partecipazione ad organismi esterni;
    iv) proposte di ricorso all'indebitamento;
    v) proposte di utilizzo di strumenti di finanza innovativa, nel rispetto della disciplina statale vigente in materia;
    vi) proposte di riconoscimento di debiti fuori bilancio e transazioni;
    vii) proposte di regolamento di contabilità, economato-provveditorato, patrimonio e di applicazione dei tributi locali;
c) vigilanza sulla regolarità contabile, finanziaria ed economica della gestione relativamente all'acquisizione delle entrate, all'effettuazione delle spese, all'attività contrattuale, all'amministrazione dei beni, alla completezza della documentazione, agli adempimenti fiscali ed alla tenuta della contabilità; l'organo di revisione svolge tali funzioni anche con tecniche motivate di campionamento;
d) relazione sulla proposta di deliberazione consiliare di approvazione del rendiconto della gestione e sullo schema di rendiconto entro il termine, previsto dal regolamento di contabilità e comunque non inferiore a 20 giorni, decorrente dalla trasmissione della

stessa proposta approvata dall'organo esecutivo. La relazione dedica un'apposita sezione all'eventuale rendiconto consolidato di cui all'articolo 11, commi 8 e 9, e contiene l'attestazione sulla corrispondenza del rendiconto alle risultanze della gestione nonché rilievi, considerazioni e proposte tendenti a conseguire efficienza, produttività ed economicità della gestione;

e) relazione sulla proposta di deliberazione consiliare di approvazione del bilancio consolidato di cui all'articolo 233-bis e sullo schema di bilancio consolidato, entro il termine previsto dal regolamento di contabilità e comunque non inferiore a 20 giorni, decorrente dalla trasmissione della stessa proposta approvata dall'organo esecutivo;

f) referto all'organo consiliare su gravi irregolarità di gestione, con contestuale denuncia ai competenti organi giurisdizionali ove si configurino ipotesi di responsabilità;

g) verifiche di cassa di cui all'articolo 223 d.lgs 267/2000.

Nei pareri di cui alla lettera b) è espresso un motivato giudizio di congruità, di coerenza e di attendibilità contabile delle previsioni di bilancio e dei programmi e progetti, anche tenuto conto dell'attestazione del responsabile del servizio finanziario ai sensi dell'articolo 153 del d.lgs.267/2000, delle variazioni rispetto all'anno precedente, dell'applicazione dei parametri di deficitarietà strutturale e di ogni altro elemento utile. Nei pareri sono suggerite all'organo consiliare le misure atte ad assicurare l'attendibilità delle impostazioni. I pareri sono obbligatori. L'organo consiliare è tenuto ad adottare i provvedimenti conseguenti o a motivare adeguatamente la mancata adozione delle misure proposte dall'organo di revisione.

Al fine di garantire l'adempimento delle funzioni di cui al precedente comma, l'organo di revisione ha diritto di accesso agli atti e documenti dell'ente e può partecipare all'assemblea dell'organo consiliare per l'approvazione del bilancio di previsione e del rendiconto di gestione. Può altresì partecipare alle altre assemblee dell'organo consiliare e, se previsto dallo statuto dell'ente, alle riunioni dell'organo esecutivo. Per consentire la partecipazione alle predette assemblee all'organo di revisione sono comunicati i relativi ordini del giorno. Inoltre all'organo di revisione sono trasmessi:

a) da parte della Corte dei conti i rilievi e le decisioni assunti a tutela della sana gestione finanziaria dell'ente;

b) da parte del responsabile del servizio finanziario le attestazioni di assenza di copertura finanziaria in ordine alle delibere di impegni di spesa.

L'organo di revisione è dotato, a cura dell'ente locale, dei mezzi necessari per lo svolgimento dei propri compiti, secondo quanto stabilito dallo statuto e dai regolamenti.
Una più dettagliata disciplina della materia è contenuta nel regolamento di contabilità.

ART. 37 - NUCLEO DI VALUTAZIONE

Il Comune di Pastrengo è dotato di un Organismo di Valutazione, di norma a composizione monocratica.
L'incarico di componente (unico o collegale) dell'Organismo di Valutazione è affidato dal Sindaco, di norma previa pubblicazione di un avviso per la presentazione delle manifestazioni di interesse.
I compiti e le funzioni dell'Organismo di Valutazione del Comune di Pastrengo sono declinati nel sistema di valutazione delle performance.

IL SISTEMA DEI PROFILI PROFESSIONALI

ART. 38 - ARTICOLAZIONE PROFILI PROFESSIONALI

I profili professionali del comune di Pastrengo, nel rispetto dei C.C.N.L. nazionali sono articolati in quattro aree:

- Area degli Operatori;
- Area degli Operatori esperti;
- Area degli Istruttori;
- Area dei Funzionari e dell'Elevata Qualificazione

I profili professionali del Comune di Pastrengo sono contenuti in apposito atto denominato: sistema dei profili professionali.

ART. 39 - PRECISAZIONI GENERALI

Tutti gli incarichi di copertura di ruoli organizzativi sono soggetti al principio di temporaneità e revocabilità.

L'attribuzione degli incarichi avviene con atto scritto del soggetto competente e va comunicato al soggetto incaricato[44] ed archiviato secondo le modalità previste dal manuale di gestone documentale e della conservazione.

Per i criteri di conferimento e di revoca, si rimanda ad un regolamento separato, da considerare quale appendice al presente, da approvare con delibera di Giunta Comunale.

ART. 40 - INCARICHI DI ELEVATA QUALIFICAZIONE

L'incarico di copertura dei ruoli individuati come di EQ sono attribuiti dal Sindaco con proprio atto.

Gli incarichi di EQ sono attribuiti, di norma, ai dipendenti o a soggetti esterni con incarico a contratto inquadrati nei profili professionali dell'area dei funzionari / EQ.

Nell'attribuzione dell'incarico di E.Q., si terrà conto dei seguenti fattori natura e caratteristiche dei programmi da realizzare;

(i) requisiti culturali posseduti;

(ii) attitudini e capacità professionali;

(iii) esperienze acquisite.

La durata degli incarichi di EQ è stabilita nel provvedimento di incarico, ma non potrà essere superiore a 3 anni

L'incarico di copertura del ruolo di EQ è rinnovabile e, di norma, segue il regime della *prorogatio*, cioè, è automaticamente prorogato fino alla successiva nomina.

Gli incarichi possono essere revocati prima della scadenza con atto scritto e motivato, in relazione a intervenuti mutamenti organizzativi o in conseguenza di valutazione negativa della performance individuale

Si applicano le disposizioni del contratto collettivo nazionale di lavoro e dei contratti collettivi decentrati integrativi.

[44] La comunicazione dell'incarico avviene di norma in forma digitale all'indirizzo mail del dipendente.

Al personale incaricato della copertura di ruoli di EQ viene riconosciuto oltre al compenso tabellare una retribuzione di posizione ed una retribuzione di risultato nei termini stabiliti dai contratti decentrati integrativi.

DOTAZIONE ORGANICA ACCESSO AGLI IMPIEGHI INCARICHI ESTERNI

ART. 42 - DOTAZIONE ORGANICA

La dotazione organica è composta dall'elenco dei profili professionali e dei relativi posti in organico distinti per posti coperti e vacanti.

ART 43 - PROGRAMMAZIONE DELLE ASSUNZIONI

I processi di assunzione del personale ed i relativi atti assunzionali sono soggetti ad una programmazione triennale, ed in ogni caso nel rispetto delle disposizioni normative vigenti tempo per tempo.

La proposta di programma assunzionale è elaborata dall'unità organizzativa che gestisce il personale (risorse umane) sulla base delle indicazioni dei Responsabili di area.

Il programma assunzionale è approvato dalla Giunta Comunale.

ART. 44 - ACCESSO AGLI IMPIEGHI

La disciplina per l'accesso agli impegni è contenuta in apposito regolamento, costituente parte dell'ordinamento generale degli uffici e dei servizi.

ART.45 - INCARICHI ESTERNI

La disciplina degli incarichi esterni è contenuta in apposito regolamento che costituisce parte integrante dell'ordinamento generale degli uffici e dei servizi

ART. 46 - DISCIPLINA DEL LAVORO AGILE

La disciplina del lavoro agile è contenuta in apposito regolamento / documento che costituisce parte integrante dell'ordinamento generale degli uffici e dei servizi.

ART. 47 DISCIPLINA DEL RAPPORTO DI LAVORO

La disciplina del rapporto di lavoro e regolata da apposito regolamento o atto organizzativo generale.

ART. 48 – UFFICIO PROCEDIMENTI DISCIPLINARI

Ai sensi del comma 2 dell'art. 55 bis del D.Lgs. 30 marzo 2001, n. 165, come modificato dall'art. 13 del D.lgs. 75/2017, l'ufficio competente per i procedimenti disciplinari (UPD) viene individuato nell'ufficio del Segretario comunale.

Tale ufficio, su segnalazione del Responsabile del servizio in cui il dipendente lavora, contesta l'addebito al dipendente medesimo, istruisce il provvedimento disciplinare e applica la sanzione.

L'Ufficio procedimenti disciplinari è integrato della figura di un segretario con funzioni di verbalizzante, svolta da un dipendente dell'Ente incardinato nell'ufficio segreteria o personale.

Quando, però, la sanzione da applicare sia il rimprovero verbale, il Responsabile del Servizio in cui il dipendente lavora provvede direttamente.

Per la contestazione di addebito nei confronti dei Responsabili di Settore provvede direttamente il Segretario Comunale.

L'Amministrazione Comunale, previa convenzione, può prevedere la gestione unificata delle funzioni dell'Ufficio per i procedimenti disciplinari con altri Enti Locali territoriali.

Per i procedimenti di particolare complessità e rilevanza, l'Ufficio per i procedimenti disciplinari può avvalersi del supporto di tecnici esterni di comprovata esperienza ed elevata professionalità in materia di contenzioso del lavoro e nei rapporti di lavoro nel pubblico impiego.

CICLO DELLA PERFOMANCE E VALUTAZIONE

ART. 49 - IL SISTEMA DI VALUTAZIONE DELLA PERFORMANCE

Il sistema di valutazione della performance è contenuto in apposito documento atto che costituisce parte integrante dell'ordinamento generale degli uffici e dei servizi.

È inserito nel sistema di valutazione della performance anche la disciplina del ciclo della performance nonché la nomina dell'Organismo di Valutazione (della performance)

Costituisce ambito della performance, e quindi è oggetto di valutazione il comportamento tenuto dai dipendenti nell'ambito dell'attività lavorativa ed il rispetto del codice di comportamento, che costituisce parte integrante dell'ordinamento generale degli uffici e dei servizi.