COMUNE DI CALENDASCO

MODELLO ORGANIZZATIVO PRIVACY

Sommario

SEZIONE I – INTRODUZIONE

1. Premessa

1.1 Il presente Modello Organizzativo relativo alla protezione dei dati personali (di seguito "**MOP**") è adottato da:

COMUNE DI CALENDASCO, con sede in 29010 Calendasco (PC), via G. Mazzini n. 4, codice fiscale 00216710335, in persona del legale rappresentante pro tempore, nella qualità di Titolare del trattamento (di seguito "**Titolare**" o "**Ente**"), al fine di definire l'assetto organizzativo e procedurale per la gestione dei trattamenti di dati personali effettuati nell'ambito dello svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico attribuiti all'Ente.

1.2 Il presente documento descrive l'organizzazione delle risorse e dei mezzi, i processi e i controlli adottati a tutela dei dati personali trattati dall'Ente nell'ambito dei procedimenti amministrativi, nonché nell'esercizio delle attività istituzionali, nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, in coerenza con gli obblighi di pubblicità, trasparenza e accessibilità previsti dalla normativa vigente.

1.3 Destinatari del presente documento sono i soggetti che, a vario titolo, partecipano allo svolgimento delle attività che comportano il trattamento di dati personali, ivi inclusi i Responsabili di servizio, i Responsabili del procedimento, il personale autorizzato al trattamento, nonché i soggetti esterni che trattano dati personali per conto dell'Ente.

2. Scopo e struttura del MOP

2.1 Il documento delinea il modello organizzativo dell'Ente in materia di protezione dei dati personali, individuando:

- i principi generali del trattamento dei dati personali nell'ambito dello svolgimento delle funzioni istituzionali;
- i ruoli e le responsabilità dei soggetti coinvolti nei trattamenti effettuati nell'ambito dei procedimenti amministrativi;
- i processi organizzativi e le misure tecniche e organizzative adottate per garantire la conformità dei trattamenti ai principi di liceità, correttezza, trasparenza, minimizzazione, limitazione della conservazione e integrità e riservatezza, tenendo conto delle specificità del contesto pubblico.

2.2 Il MOP è strutturato in sezioni corrispondenti ai principali ambiti di conformità individuati dalla normativa in materia di protezione dei dati personali, come di seguito schematizzati:

- definizione del perimetro di applicazione del MOP e del contesto operativo dell'Ente;
- individuazione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento dei dati personali;
- garanzia dei diritti degli interessati e diffusione di adeguate informazioni in merito ai trattamenti effettuati, anche in relazione agli obblighi normativi in materia di pubblicità

legale, trasparenza amministrativa e diritto di accesso ai documenti amministrativi e civico generalizzato;

> adozione di misure tecniche e organizzative idonee a dimostrare la conformità ai principi applicabili al trattamento dei dati personali, anche mediante la mappatura delle attività di trattamento, la valutazione dei rischi per gli interessati, la determinazione dei tempi di conservazione dei dati personali e la gestione degli incidenti di sicurezza;

> coordinamento tra le esigenze di protezione dei dati personali e gli obblighi normativi in materia di pubblicità legale, trasparenza amministrativa e diritto di accesso ai documenti amministrativi e civico generalizzato.

3. Contesto normativo e regolamentare

3.1 Il MOP è conforme:

> ai principi stabiliti dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "GDPR");

> alle disposizioni del D. Lgs. 30 giugno 2003, n. 196, così come modificato e integrato dal D. Lgs. 10 agosto 2018, n. 101 ("Codice in materia di protezione dei dati personali");

> alla normativa nazionale e settoriale che disciplina lo svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico attribuiti all'Ente, e che costituisce base giuridica del trattamento dei dati personali ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR e dell'art. 2-ter del Codice in materia di protezione dei dati personali;

> alla normativa vigente in materia di formazione, gestione e conservazione dei documenti amministrativi e informatici, nonché di gestione degli archivi pubblici;

> alla normativa vigente in materia di pubblicità legale, trasparenza amministrativa e diritto di accesso ai documenti amministrativi e ai dati detenuti dalle pubbliche amministrazioni.

3.2 Il presente documento è regolarmente adeguato e aggiornato in relazione agli eventuali mutamenti normativi, regolamentari e organizzativi che incidono sulle modalità di trattamento dei dati personali effettuati dall'Ente.

4. Formazione del personale e diffusione del documento

4.1 L'Ente promuove la conoscenza del MOP tra i soggetti che, a vario titolo, partecipano allo svolgimento di attività che comportano il trattamento di dati personali, inclusi i

Responsabili di servizio, i Responsabili del procedimento e il personale autorizzato al trattamento.

A tal fine, l'Ente assicura l'adozione di adeguate iniziative di formazione e aggiornamento in materia di protezione dei dati personali, in relazione ai compiti e alle responsabilità attribuiti nell'ambito dei procedimenti amministrativi.

La formazione in materia di protezione dei dati personali costituisce misura organizzativa ai sensi dell'art. 32 del GDPR ed è finalizzata a garantire che il trattamento dei dati personali avvenga nel rispetto dei principi di liceità, correttezza, trasparenza e minimizzazione, nonché in conformità agli obblighi normativi in materia di pubblicità legale, trasparenza amministrativa e diritto di accesso.

5. Definizioni principali in materia di protezione dei dati personali

5.1 Di seguito si forniscono le definizioni principali in materia di protezione dei dati personali:

a. "**dato personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Tra i dati personali ve ne sono alcuni che, per loro natura, debbono essere trattati con particolari cautele. Questi sono quelli rientranti in:

a.1 "**categorie particolari di dati personali**", vale a dire quei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona. In particolare, in questa categoria rientrano i "dati genetici", cioè i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; i "dati biometrici": cioè i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; i "dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

a.2 "**dati personali relativi a condanne penali e reati**" o "**dati giudiziari**", vale a dire quei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

b. "**trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c. "**archivio**": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

d. "**Titolare del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

e. "**Responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

f. "**autorizzati al trattamento**": persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare del trattamento o del Responsabile del trattamento;

g. "**destinatario**": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;

h. "**terzo**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

i. "**consenso dell'interessato**": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

j. "**violazione dei dati personali**": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

k. "**misure di sicurezza**": misure tecniche e organizzative adeguate per garantire un livello di sicurezza e di protezione dei dati personali adeguato al rischio di distruzione, perdita, accesso non autorizzato, trattamento non consentito o non conforme, ecc.

l. "**Autorità di controllo**": l'autorità pubblica indipendente, vale a dire il "Garante per la protezione dei dati Personali".

6. Principi generali sul trattamento dei dati personali

6.1 Qualsiasi attività di trattamento di dati personali effettuata dall'Ente avviene nel rispetto dei principi di cui all'art. 5 del Regolamento (UE) 2016/679, e in particolare dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione e integrità e riservatezza.

6.2 Il trattamento dei dati personali è lecito quando necessario per l'adempimento di un obbligo legale al quale è soggetto il Titolare o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri attribuiti all'Ente dalla normativa vigente, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR e dell'art. 2-ter del Codice in materia di protezione dei dati personali.

6.3 Fatto salvo quanto sopra, ulteriori trattamenti di dati personali non strettamente necessari allo svolgimento delle funzioni istituzionali possono essere effettuati dall'Ente sulla base di altre condizioni di liceità previste dall'art. 6 del GDPR, nei limiti e alle condizioni stabilite dalla normativa vigente.

6.4 Il trattamento dei dati personali deve essere limitato a quanto necessario per lo svolgimento delle funzioni istituzionali attribuite all'Ente e per la gestione dei procedimenti amministrativi di competenza, nel rispetto delle finalità determinate dalla normativa di settore.

6.5 I dati personali sono trattati in modo da garantire un adeguato livello di sicurezza, mediante l'adozione di misure tecniche e organizzative idonee a prevenire il rischio di distruzione, perdita, accesso non autorizzato o trattamento non consentito.

6.6 Il trattamento dei dati personali è effettuato tenendo conto della necessità di garantire un adeguato bilanciamento tra la tutela dei diritti e delle libertà fondamentali degli interessati e gli obblighi normativi in materia di pubblicità legale, trasparenza amministrativa e diritto di accesso ai documenti amministrativi.

SEZIONE II – CONTESTO

7. Contesto operativo

7.1 Nell'ambito dello svolgimento delle proprie funzioni istituzionali e dei compiti di interesse pubblico attribuiti dalla normativa vigente, l'Ente può effettuare trattamenti di dati personali su supporto cartaceo e informatico, anche mediante strumenti automatizzati, riguardanti diverse categorie di interessati, quali cittadini, utenti dei servizi, dipendenti, collaboratori, fornitori e altri soggetti che interagiscono con l'Ente. I trattamenti possono essere effettuati, a titolo esemplificativo e non esaustivo, nell'ambito delle attività connesse alla gestione dei servizi demografici, dei tributi, dei servizi sociali, della polizia locale, dell'istruzione e degli altri servizi istituzionali erogati dall'Ente.

7.2 Tali trattamenti possono riguardare dati personali comuni, nonché, ove necessario per lo svolgimento dei compiti istituzionali attribuiti all'Ente, categorie particolari di dati personali e dati relativi a condanne penali e reati.

7.3 Il trattamento dei dati personali è effettuato nel rispetto dei principi di cui all'art. 5 del GDPR ed è limitato a quanto necessario per lo svolgimento delle funzioni istituzionali e per la gestione dei procedimenti amministrativi di competenza dell'Ente.

7.4 In relazione ai trattamenti effettuati nell'ambito delle attività istituzionali, la base giuridica del trattamento è costituita dall'adempimento di un obbligo legale al quale è soggetto il Titolare o dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri attribuiti all'Ente dalla normativa vigente, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR e dell'art. 2-*ter* del Codice in materia di protezione dei dati personali.

7.5 Il trattamento di categorie particolari di dati personali è effettuato esclusivamente nei casi previsti dalla normativa vigente e, in particolare, quando necessario per motivi di interesse pubblico rilevante, ai sensi dell'art. 9, par. 2, lett. g) del GDPR e delle disposizioni di legge applicabili.

7.6 Ulteriori trattamenti di dati personali non strettamente necessari allo svolgimento delle funzioni istituzionali possono essere effettuati dall'Ente sulla base di altre condizioni di liceità previste dall'art. 6 del GDPR, nei limiti e alle condizioni stabilite dalla normativa vigente.

7.7 Il trattamento dei dati personali dei dipendenti e dei collaboratori dell'Ente è effettuato per le finalità connesse all'instaurazione e alla gestione del rapporto di lavoro o di servizio, nonché per l'adempimento degli obblighi previsti dalla normativa vigente in materia di diritto del lavoro, sicurezza sociale e tutela della salute e sicurezza nei luoghi di lavoro.

7.8 Il trattamento dei dati personali di fornitori, consulenti e altri soggetti che intrattengono rapporti giuridici con l'Ente è effettuato per finalità connesse alla gestione dei rapporti contrattuali e all'adempimento dei relativi obblighi normativi e amministrativi.

7.9 Qualora l'Ente effettui trattamenti di dati personali ulteriori rispetto a quelli necessari allo svolgimento delle funzioni istituzionali, tali trattamenti possono essere fondati sul consenso dell'interessato nei casi previsti dalla normativa vigente, fermo restando che il consenso costituisce base giuridica del trattamento esclusivamente quando lo stesso non sia necessario per l'adempimento di obblighi legali o per l'esecuzione di compiti di interesse pubblico.

SEZIONE III- SOGGETTI

8. Ruoli e responsabilità

8.1 La realizzazione di un idoneo sistema di protezione dei dati personali richiede l'individuazione dei soggetti coinvolti nelle attività di trattamento, nonché la definizione dei

rispettivi ruoli, compiti e responsabilità nell'ambito dello svolgimento delle funzioni istituzionali e dei procedimenti amministrativi di competenza dell'Ente.

8.2 La gestione dei trattamenti di dati personali effettuati dall'Ente è attribuita al Titolare del trattamento, che opera attraverso le proprie strutture organizzative, in conformità alle disposizioni normative vigenti e nel rispetto delle competenze attribuite ai Responsabili di servizio e ai Responsabili del procedimento.

8.3 Nell'ambito della propria organizzazione, l'Ente individua i soggetti che, a vario titolo, partecipano allo svolgimento delle attività che comportano il trattamento di dati personali, tra cui:

- i Responsabili di servizio;
- i Responsabili del procedimento;
- i soggetti designati per specifici compiti e funzioni;
- le persone autorizzate al trattamento;
- i Responsabili del trattamento;
- il Responsabile della protezione dei dati personali ("Data Protection Officer" o "DPO").

8.4 Le persone fisiche a cui si riferiscono i dati personali trattati sono gli "interessati", i quali beneficiano delle tutele previste dalla normativa vigente in materia di protezione dei dati personali.

8.5 L'Ente può individuare una funzione interna di supporto organizzativo in materia di protezione dei dati personali (di seguito "Referente privacy"), con compiti di coordinamento operativo delle attività connesse all'attuazione del presente Modello Organizzativo Privacy. Il Referente privacy supporta il Titolare del trattamento e le strutture organizzative dell'Ente nella diffusione delle procedure interne, nel monitoraggio delle misure adottate e nella gestione degli adempimenti connessi alla protezione dei dati personali, fermo restando che la determinazione delle finalità e dei mezzi del trattamento resta attribuita ai soggetti competenti nell'ambito dei procedimenti amministrativi. Il Referente privacy opera in raccordo con il Responsabile della protezione dei dati personali (DPO), nel rispetto dei rispettivi ruoli e responsabilità.

9. Titolare del trattamento

9.1 Il Titolare del trattamento 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 ai sensi dell'art. 4, par. 1, punto 7 del GDPR.

9.2 Nell'ambito del presente MOP, l'Ente è identificato quale Titolare del trattamento dei dati personali effettuati nello svolgimento delle proprie funzioni istituzionali.

9.3 Il Titolare del trattamento esercita le proprie competenze in materia di protezione dei dati personali attraverso le strutture organizzative dell'Ente, in conformità all'ordinamento degli enti locali e nel rispetto delle competenze attribuite agli organi di governo, ai dirigenti o ai Responsabili di servizio e ai Responsabili del procedimento.

9.4 Nell'ambito della propria organizzazione interna, il Titolare del trattamento, tra l'altro:

- determina le finalità e i mezzi del trattamento dei dati personali;
- garantisce l'adozione di misure tecniche e organizzative adeguate per assicurare la sicurezza del trattamento, anche in applicazione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita;
- assicura l'idonea formazione del personale autorizzato al trattamento;
- procede, ove necessario, alla valutazione d'impatto sulla protezione dei dati personali (DPIA);
- tiene il Registro delle attività di trattamento svolte sotto la propria responsabilità;
- nomina i Responsabili del trattamento e ne verifica l'operato;
- designa il Responsabile della protezione dei dati personali (DPO) e coopera con lo stesso, garantendone l'indipendenza;
- cura la notifica di eventuali violazioni dei dati personali all'Autorità di controllo e, ove necessario, agli interessati;
- fornisce adeguato riscontro alle richieste degli interessati nell'esercizio dei diritti previsti dalla normativa vigente;
- coopera con l'Autorità di controllo.

11. Designati per specifici compiti e funzioni

11.1 In considerazione della complessità della struttura e dell'organizzazione interna, il Titolare del trattamento, ai sensi dell'art. 2-*quaterdecies*, comma 1, del Codice in materia di protezione dei dati personali e nell'ambito del proprio assetto organizzativo, può designare persone fisiche cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali.

11.2 La designazione è formalizzata per iscritto, con indicazione delle istruzioni impartite e individuazione dei compiti e delle responsabilità attribuiti nell'ambito delle attività di trattamento dei dati personali.

11.3 I soggetti designati per specifici compiti e funzioni operano nell'ambito della struttura organizzativa di appartenenza e svolgono le attività connesse al trattamento dei dati personali in conformità alle istruzioni impartite dal Titolare del trattamento.

11.4 In particolare, ai soggetti designati possono essere attribuiti, nell'ambito della propria struttura di competenza, i seguenti compiti:

- assicurare l'attuazione delle istruzioni, direttive, policy e procedure in materia di protezione dei dati personali fornite dal Titolare del trattamento;
- collaborare all'individuazione e all'adozione delle misure tecniche e organizzative idonee a garantire la sicurezza dei dati personali trattati;
- vigilare sull'osservanza, da parte delle persone autorizzate al trattamento, delle istruzioni impartite dal Titolare;
- collaborare alla gestione e all'aggiornamento del Registro delle attività di trattamento;
- segnalare tempestivamente al Titolare del trattamento eventuali richieste di esercizio dei diritti da parte degli interessati e collaborare alle relative istruttorie;
- segnalare tempestivamente al Titolare del trattamento eventuali violazioni dei dati personali o situazioni di rischio;
- collaborare con il Responsabile della protezione dei dati personali (DPO) fornendo le informazioni richieste;
- proporre l'individuazione di soggetti esterni da nominare quali Responsabili del trattamento ai sensi dell'art. 28 del GDPR e supportare le relative attività istruttorie.

11.5 I soggetti designati possono altresì proporre al Titolare del trattamento soluzioni organizzative e tecniche idonee a migliorare la sicurezza dei dati personali trattati, nonché segnalare eventuali fabbisogni formativi in materia di protezione dei dati personali.

11.6 I soggetti designati operano sotto l'autorità del Titolare del trattamento e non determinano in autonomia le finalità e i mezzi del trattamento dei dati personali.

12. Autorizzati al trattamento dei dati personali

12.1 Gli autorizzati al trattamento dei dati personali sono le persone fisiche che, operando sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento, effettuano materialmente operazioni di trattamento di dati personali ai sensi dell'art. 4, par. 1, punto 10 del GDPR e dell'art. 2-*quaterdecies*, comma 1 del Codice in materia di protezione dei dati personali. Si tratta dei dipendenti e dei collaboratori dell'Ente che, nell'esercizio delle proprie mansioni, trattano dati personali.

12.2 Gli autorizzati operano sotto l'autorità del Titolare del trattamento e dei soggetti designati per specifici compiti e funzioni nell'ambito della struttura organizzativa di appartenenza e sono tenuti a rispettare le istruzioni impartite.

12.3 L'autorizzazione è circoscritta al trattamento dei soli dati personali necessari allo svolgimento dei compiti assegnati, in conformità alle mansioni attribuite.

12.4 Gli autorizzati che vengano a conoscenza di una violazione dei dati personali o di un incidente che coinvolga dati personali sono tenuti a darne tempestiva comunicazione al soggetto designato per specifici compiti e funzioni o al proprio responsabile gerarchico.

12.5 L'individuazione degli autorizzati avviene mediante atto di designazione formalizzato per iscritto, recante le istruzioni per il trattamento dei dati personali.

13. Responsabili del trattamento

13.1 Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento ai sensi dell'art. 4, par. 1, punto 8 del GDPR.

13.2 Il Responsabile del trattamento è il soggetto che gestisce o compie operazioni di trattamento di dati personali per conto del Titolare del trattamento.

13.3 Ai sensi dell'art. 28, par. 1 del GDPR, il Titolare impiega unicamente Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti degli interessati.

13.4 La designazione del Responsabile del trattamento è necessaria quando il Titolare affida a soggetti esterni lo svolgimento di attività che comportano il trattamento di dati personali per suo conto, salvo che tali soggetti operino in qualità di autonomi Titolari del trattamento.

13.5 I trattamenti effettuati da un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico, che definisce oggetto, durata, natura e finalità del trattamento, il tipo di dati personali e le categorie di interessati, nonché gli obblighi e i diritti del Titolare del trattamento.

13.6 Il Responsabile del trattamento tratta i dati personali soltanto su istruzioni documentate del Titolare del trattamento e adotta tutte le misure tecniche e organizzative adeguate a garantire la sicurezza del trattamento ai sensi dell'art. 32 del GDPR.

13.7 I Responsabili del trattamento esterni costituiscono parte integrante dell'assetto organizzativo dei trattamenti effettuati dall'Ente per le attività esternalizzate.

13.8 La designazione del Responsabile del trattamento è formalizzata per iscritto mediante atto di nomina o accordo sul trattamento dei dati personali.

13.9 Il Titolare del trattamento può effettuare attività di valutazione e monitoraggio volte a verificare l'adeguatezza delle misure tecniche e organizzative adottate dai Responsabili del trattamento.

13.10 Le attività di valutazione possono essere effettuate anche mediante la somministrazione di questionari o checklist in sede di prequalifica o di verifica periodica.

13.11 L'Ente, in qualità di Titolare del trattamento, individua i soggetti che trattano dati personali per suo conto e, ove necessario, provvede alla loro designazione quali Responsabili del trattamento ai sensi dell'art. 28 del GDPR.

13.12 Nell'ambito dei rapporti con soggetti esterni che, nello svolgimento delle attività affidate, possano trovarsi a trattare dati personali, si rinvia alla specifica **procedura per l'inquadramento del ruolo privacy dei fornitori e la conseguente formalizzazione dei rapporti di trattamento,** che definisce criteri, strumenti operativi e modalità di valutazione ai fini della corretta qualificazione dei medesimi quali Titolari autonomi, Responsabili del trattamento o Contitolari, nel rispetto delle disposizioni del GDPR e del principio di responsabilizzazione.

15. Responsabile della protezione dei dati personali

15.1 Il Responsabile della protezione dei dati personali ("Data Protection Officer" o "DPO") è una figura prevista dagli artt. 37 e seguenti del GDPR.

15.2 Il Responsabile della protezione dei dati personali è nominato dal Titolare del trattamento per assolvere a funzioni di supporto, controllo, consultive, formative e informative relativamente all'applicazione della normativa in materia di protezione dei dati personali.

15.3 La designazione del Responsabile della protezione dei dati personali è obbligatoria per le autorità pubbliche e gli organismi pubblici ai sensi dell'art. 37, par. 1, lett. a) del GDPR.

15.4 Il Responsabile della protezione dei dati personali deve:

- essere in possesso di un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- adempiere alle proprie funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del Titolare del trattamento oppure sulla base di un contratto di servizio.

15.5 Il Responsabile della protezione dei dati personali svolge almeno i seguenti compiti:

- informare e fornire consulenze al Titolare del trattamento e al personale che esegue trattamenti di dati personali in merito alla disciplina in materia di protezione dei dati personali;
- sorvegliare l'osservanza della normativa in materia e delle politiche del Titolare relative alla protezione dei dati personali;
- fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati personali e sorvegliarne lo svolgimento;

- fungere da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati personali.

15.6 Il Titolare del trattamento mette a disposizione del Responsabile della protezione dei dati personali le risorse necessarie per adempiere ai propri compiti e accedere ai dati personali e ai trattamenti.

15.7 Il ruolo di Responsabile della protezione dei dati personali può essere ricoperto da un soggetto interno all'organizzazione oppure da un soggetto esterno.

15.8 Il nominativo del Responsabile della protezione dei dati personali e i relativi dati di contatto sono resi pubblici e comunicati al Garante per la protezione dei dati personali.

15.9 L'Ente provvede alla designazione del Responsabile della protezione dei dati personali ai sensi degli artt. 37 e seguenti del GDPR.

16. Organigramma privacy

16.1 L'Ente redige e mantiene aggiornato l'organigramma privacy in relazione a eventuali modifiche organizzative.

SEZIONE IV – DIRITTI DEGLI INTERESSATI

17. Gli interessati ed i loro diritti

17.1 Le persone fisiche cui si riferiscono i dati personali trattati dal Titolare sono gli "interessati", destinatari delle tutele previste dalla normativa in materia di protezione dei dati personali.

17.2 Tali tutele si sostanziano nel diritto a ricevere adeguate informative e comunicazioni relativamente ai trattamenti svolti dal Titolare, nonché ad esercitare i diritti previsti dagli artt. da 15 a 22 del GDPR.

17.3 Nei casi previsti dalla normativa vigente, gli interessati possono altresì esprimere il consenso al trattamento dei dati personali che li riguardano, qualora tale trattamento non sia fondato sull'adempimento di un obbligo legale o sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

17.4 Gli interessati possono esercitare nei confronti del Titolare una serie di diritti finalizzati a conoscere, verificare, modificare o aggiornare i dati personali che li riguardano, nei limiti previsti dalla normativa vigente.

17.5 Ai sensi degli artt. da 15 a 22 del GDPR, gli interessati possono:

- ottenere la conferma che sia o meno in corso un trattamento di dati personali che li riguardano e accedere agli stessi (“diritto di accesso”);
- ottenere la rettifica dei dati personali inesatti che li riguardano (“diritto di rettifica”);
- ottenere, nei casi previsti dalla normativa vigente, la cancellazione dei dati personali (“diritto alla cancellazione”);
- ottenere la limitazione del trattamento (“diritto di limitazione del trattamento”);
- esercitare il diritto alla portabilità dei dati, nei casi previsti dall’art. 20 del GDPR;
- revocare il consenso eventualmente prestato, nei casi in cui il trattamento sia fondato su tale base giuridica;
- opporsi al trattamento dei dati personali nei casi previsti dall’art. 21 del GDPR;
- proporre reclamo all’Autorità di controllo competente o adire le opportune sedi giudiziarie.

17.6 L’esercizio dei diritti da parte degli interessati può essere limitato nei casi previsti dall’art. 23 del GDPR e dalla normativa nazionale vigente, qualora dal relativo esercizio possa derivare un pregiudizio effettivo e concreto allo svolgimento di compiti di interesse pubblico o all’adempimento di obblighi di legge cui è soggetto il Titolare del trattamento.

17.7 In particolare, i diritti di cui agli artt. da 15 a 22 del GDPR possono subire limitazioni qualora il trattamento sia necessario per finalità di archiviazione nel pubblico interesse, in conformità alla normativa vigente in materia di documentazione amministrativa e conservazione degli atti.

17.8 Il Titolare del trattamento adotta misure adeguate a fornire, in forma concisa, trasparente, intelligibile e facilmente accessibile, tutte le informazioni necessarie a dare seguito alle istanze degli interessati.

17.9 Il Titolare può non dare seguito alle richieste degli interessati qualora non sia in grado di identificarli oppure qualora le richieste risultino manifestamente infondate o eccessive.

17.10 Il Titolare fornisce riscontro alle richieste degli interessati senza ingiustificato ritardo e, comunque, entro un mese dal ricevimento dell’istanza, salvo proroga nei casi previsti dall’art. 12 del GDPR.

17.11 Il Titolare informa l’interessato di eventuali limitazioni o del mancato accoglimento della richiesta, indicando le motivazioni e la possibilità di proporre reclamo all’Autorità di controllo o ricorso giurisdizionale.

17.12 È prevista una **procedura specifica per la gestione delle richieste di esercizio dei diritti da parte degli interessati**.

18. Dati personali e obblighi di pubblicità legale, trasparenza e diritto di accesso

18.1 Nell'ambito delle proprie attività istituzionali, l'Ente effettua trattamenti di dati personali anche in adempimento degli obblighi normativi in materia di pubblicità legale, trasparenza amministrativa e diritto di accesso ai documenti amministrativi e civico generalizzato.

18.2 In tali casi, il trattamento dei dati personali è effettuato nel rispetto dei principi di cui all'art. 5 GDPR e sulla base delle disposizioni normative applicabili, assicurando il necessario bilanciamento tra le esigenze di conoscibilità dell'azione amministrativa e la tutela dei diritti e delle libertà fondamentali degli interessati, anche alla luce delle **Linee guida adottate dall'Autorità Garante per la protezione dei dati personali in materia di trattamento di dati personali effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web**.

18.3 L'Ente adotta misure tecniche e organizzative idonee a limitare la diffusione o la comunicazione dei dati personali non pertinenti o eccedenti rispetto alle finalità di pubblicità, trasparenza o ostensione, anche mediante l'oscuramento selettivo delle informazioni contenute negli atti oggetto di pubblicazione o accesso.

SEZIONE V – ACCOUNTABILITY

19. Registri delle attività di trattamento

19.1 L'Ente, in qualità di Titolare del trattamento, tiene il Registro delle attività di trattamento, in forma scritta, anche in formato elettronico, relativo ai trattamenti svolti sotto la propria responsabilità.

19.2 Il Registro delle attività di trattamento è mantenuto aggiornato e messo a disposizione del Garante per la protezione dei dati personali su richiesta.

19.3 Ai sensi dell'art. 30, par. 1 del GDPR, il Registro del Titolare contiene almeno le seguenti informazioni:

- il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati;
- le finalità dei trattamenti;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative applicate.

19.4 Qualora l'Ente tratti dati personali per conto di un altro Titolare del trattamento, esso tiene un Registro delle attività di trattamento svolte in qualità di Responsabile, ai sensi dell'art. 30, par. 2 del GDPR.

19.5 Il Registro delle attività di trattamento è aggiornato periodicamente e comunque in occasione di modifiche organizzative, procedurali o tecnologiche che incidano sui trattamenti effettuati.

19.6 L'aggiornamento delle informazioni contenute nel Registro delle attività di trattamento è effettuato dalle strutture organizzative competenti nell'ambito dei rispettivi procedimenti amministrativi. Il Referente privacy, ove individuato, assicura il coordinamento operativo delle attività di raccolta e aggiornamento delle informazioni necessarie alla tenuta del Registro.

20. Valutazione di impatto sulla protezione dei dati personali

20.1 Qualora un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità dello stesso, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Ente effettua, prima di procedere al trattamento, una valutazione di impatto sulla protezione dei dati personali ("Data Protection Impact Assessment" o "DPIA"), ai sensi dell'art. 35 del GDPR.

20.2 La DPIA è una procedura che mira a descrivere il trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché i relativi rischi, allo scopo di individuare le misure idonee a mitigarli.

20.3 La DPIA costituisce uno strumento di responsabilizzazione in quanto consente al Titolare del trattamento di valutare e dimostrare la conformità del trattamento alle disposizioni in materia di protezione dei dati personali.

20.4 La DPIA è richiesta in particolare nei casi previsti dall'art. 35 del GDPR e dal Provvedimento del Garante per la protezione dei dati personali n. 467 dell'11 ottobre 2018.

20.5 La DPIA contiene almeno:

- una descrizione sistematica dei trattamenti previsti e delle relative finalità;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, incluse le garanzie e le misure di sicurezza adottate.

20.6 Qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare tale rischio, l'Ente procede, prima di avviare il trattamento, alla consultazione preventiva del Garante per la protezione dei dati personali ai sensi dell'art. 36 del GDPR.

21. Sicurezza nel trattamento dei dati personali: analisi e valutazione dei rischi

21.1 La valutazione dei rischi costituisce elemento centrale del processo di responsabilizzazione del Titolare del trattamento.

21.2 L'analisi dei rischi è finalizzata all'adozione di misure tecniche e organizzative adeguate ai sensi dell'art. 32 del GDPR e tiene conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

21.3 La valutazione del rischio è effettuata con riferimento agli effetti che il trattamento può determinare sugli interessati, tenendo conto, tra l'altro, del rischio di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

21.4 Ai fini dell'individuazione del livello di rischio, sono considerati, tra gli altri, l'origine, la natura, la gravità e la probabilità dell'impatto sui diritti e le libertà degli interessati.

22. Metodologia per l'analisi e la valutazione del rischio

22.1 L'Ente adotta un approccio basato sul rischio ("risk-based approach") ai fini dell'individuazione e dell'implementazione di misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali trattati.

22.2 L'analisi e la valutazione del rischio sono effettuate tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà delle persone fisiche.

22.3 Ai fini della valutazione del rischio, l'Ente può avvalersi di metodologie e standard riconosciuti a livello nazionale o internazionale, quali, a titolo esemplificativo, le linee guida elaborate dall'Agenzia europea per la sicurezza delle reti e delle informazioni (ENISA) o altri modelli di analisi del rischio applicabili al contesto organizzativo dell'Ente.

22.4 Le metodologie adottate per l'analisi e la valutazione del rischio, nonché i relativi criteri di stima della probabilità e dell'impatto, sono definiti in specifici documenti tecnici interni, soggetti ad aggiornamento periodico.

22.5 In esito alla valutazione del rischio, l'Ente individua e attua le misure tecniche e organizzative adeguate al livello di rischio individuato, al fine di garantire la sicurezza dei dati personali trattati ai sensi dell'art. 32 del GDPR.

23. Sicurezza nel trattamento dei dati personali: misure di sicurezza

23.1 L'Ente adotta misure tecniche e organizzative adeguate a garantire un livello di sicurezza dei dati personali adeguato al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento.

23.2 Le misure di sicurezza sono individuate e implementate in applicazione del principio di protezione dei dati fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default), ai sensi dell'art. 25 del GDPR.

23.3 Il trattamento dei dati personali è effettuato in modo da garantire la sicurezza degli stessi, mediante misure idonee a prevenire trattamenti non autorizzati o illeciti, nonché la perdita, la distruzione o il danno accidentale dei dati.

23.4 Ai sensi dell'art. 32 del GDPR, le misure di sicurezza sono approntate tenendo conto del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

23.5 Le misure di sicurezza comprendono misure tecniche e organizzative finalizzate a garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati.

23.6 In particolare, le misure di sicurezza sono volte a garantire che:

i dati personali siano accessibili esclusivamente ai soggetti autorizzati;

i dati personali siano esatti e aggiornati rispetto alle finalità del trattamento;

i dati personali siano disponibili e accessibili in caso di incidente fisico o tecnico, anche mediante idonei sistemi di backup e continuità operativa.

23.7 L'Ente adotta altresì misure di sicurezza di natura organizzativa e procedurale finalizzate a prevenire accessi non autorizzati o utilizzi impropri dei sistemi informativi e degli strumenti di lavoro utilizzati per il trattamento dei dati personali.

23.8 Le misure di sicurezza tecniche e organizzative adottate dall'Ente sono definite in specifici documenti e policy interne, soggetti ad aggiornamento periodico, anche tenendo conto di standard e linee guida nazionali ed europee in materia di sicurezza delle informazioni, quali, a titolo esemplificativo, il Vademecum per la Pubblica Amministrazione in materia di cybersicurezza predisposto dall'Agenzia per la Cybersicurezza Nazionale (ACN) in collaborazione con il Dipartimento della Funzione Pubblica.

23.9 L'Ente adotta specifiche policy organizzative finalizzate a prevenire trattamenti non autorizzati o illeciti di dati personali e a garantire la disponibilità delle informazioni trattate mediante strumenti informatici. In particolare, sono adottate la **policy di utilizzo consapevole degli strumenti informatici, della posta elettronica e della rete Internet**, volta a ridurre il rischio di incidenti di sicurezza derivanti da comportamenti non conformi del personale, nonché la **policy per la gestione degli account istituzionali e la continuità operativa dei servizi digitali**, finalizzata a garantire la disponibilità dei dati personali trattati anche in caso di indisponibilità dell'utente o cessazione del rapporto di lavoro.

23.10 Tali policy costituiscono misure organizzative ai sensi dell'art. 32 del GDPR.

24. Periodo di conservazione dei dati personali

24.1 I dati personali trattati dall'Ente sono conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati e, comunque, nel rispetto degli obblighi di conservazione previsti dalla normativa vigente.

24.2 Nel contesto dell'attività amministrativa dell'Ente, la determinazione dei tempi di conservazione dei dati personali è effettuata tenendo conto, in via prioritaria, degli obblighi di conservazione dei documenti amministrativi previsti dalla normativa di settore, nonché delle disposizioni in materia di archiviazione nel pubblico interesse, anche ai sensi del Codice dei beni culturali e del paesaggio e delle Linee guida in materia di formazione, gestione e conservazione dei documenti informatici adottate dall'Agenzia per l'Italia Digitale (AgID).

24.3 I dati personali contenuti in documenti amministrativi sono pertanto conservati per il tempo previsto dai piani di classificazione e dai massimari di selezione e scarto adottati dall'Ente, fatti salvi eventuali obblighi di conservazione ulteriori previsti dalla normativa vigente.

24.4 Al termine dei periodi di conservazione previsti, i dati personali sono oggetto di cancellazione, anonimizzazione o distruzione, ove compatibile con gli obblighi di conservazione documentale e di archiviazione nel pubblico interesse.

24.5 L'Ente adotta specifiche **policy e procedure in materia di conservazione e scarto dei documenti contenenti dati personali (Data Retention)**, in coerenza con il sistema di gestione documentale e con il principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), GDPR.

25. Raccordo con il sistema di gestione documentale e archivistico

25.1 Ai fini dell'attuazione del principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), GDPR, l'Ente assicura il raccordo tra il sistema di protezione dei dati personali e il sistema di gestione documentale e archivistico.

25.2 In particolare, l'individuazione dei tempi di conservazione dei dati personali trattati nell'ambito dell'attività amministrativa è effettuata in coerenza con:

- il piano di classificazione (titolario);
- il piano di fascicolazione;
- il massimario di selezione e scarto;
- il piano di conservazione adottati dall'Ente ai sensi della normativa vigente in materia di gestione documentale e archivi.

25.3 L'avvio del processo archivistico, mediante classificazione e fascicolazione dei documenti contenenti dati personali, costituisce misura organizzativa idonea a garantire la corretta determinazione dei tempi di conservazione e l'attuazione delle operazioni di selezione e scarto.

25.4 Le operazioni di conservazione, selezione e scarto dei documenti contenenti dati personali sono effettuate nel rispetto:

- della normativa in materia di archivi e documentazione amministrativa;
- delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici;
- del principio di responsabilizzazione di cui all'art. 5, par. 2, GDPR.

25.5 Il Titolare del trattamento assicura che le procedure di gestione documentale e archivistica siano integrate nel sistema di gestione della protezione dei dati personali, al fine di garantire che i dati personali siano conservati per un periodo non superiore a quello necessario rispetto alle finalità per le quali sono trattati, fatte salve le esigenze di archiviazione nel pubblico interesse.

26. Violazioni di dati personali ("data breach")

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

26.2 Una violazione dei dati personali può compromettere la:

- riservatezza (accesso o divulgazione non autorizzata);
- integrità (alterazione non autorizzata);
- disponibilità (perdita o distruzione);

dei dati personali trattati.

26.3 A titolo esemplificativo, possono costituire violazione di dati personali:

- l'accesso o l'acquisizione dei dati da parte di soggetti non autorizzati;
- il furto o la perdita di dispositivi contenenti dati personali;
- l'alterazione non autorizzata di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o attacchi informatici;
- la perdita o distruzione di dati personali a causa di eventi avversi o calamità;
- la divulgazione non autorizzata di dati personali.

26.4 Al verificarsi di un incidente di sicurezza che possa comportare una violazione di dati personali, il personale autorizzato al trattamento è tenuto a darne tempestiva comunicazione al Designato per specifici compiti e funzioni della struttura organizzativa di appartenenza, secondo quanto previsto dalla procedura interna di gestione degli incidenti. Il Designato provvede a informare senza ritardo il Titolare del trattamento e il Responsabile della protezione dei dati personali, ai fini delle valutazioni di competenza.

26.5 Il Titolare del trattamento valuta, senza ingiustificato ritardo, se la violazione sia suscettibile di presentare un rischio per i diritti e le libertà delle persone fisiche.

26.6 Qualora la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare notifica la violazione al Garante per la protezione dei dati personali, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

26.7 Qualora la notifica non sia effettuata entro il termine di 72 ore, essa è accompagnata dai motivi del ritardo.

26.8 Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione anche agli interessati, salvo che siano state adottate misure tecniche e organizzative idonee a ridurne l'impatto.

26.9 Il Titolare documenta tutte le violazioni dei dati personali, indipendentemente dall'obbligo di notifica all'Autorità di controllo, ai fini della dimostrazione del rispetto della normativa applicabile.

26.10 È prevista una specifica **procedura interna per la gestione degli incidenti di sicurezza e delle violazioni di dati personali (Data Breach)**.

27. Gestione dei controlli in materia di protezione dei dati personali

27.1 Il Titolare del trattamento pianifica ed esegue attività di controllo e monitoraggio in materia di protezione dei dati personali, finalizzate a verificare l'effettiva attuazione delle misure tecniche e organizzative adottate.

27.2 I controlli possono riguardare:

- gli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali;
- i trattamenti censiti nei Registri delle attività di trattamento;
- l'operato degli autorizzati al trattamento;
- l'operato dei Responsabili del trattamento.

27.3 La pianificazione dei controlli è effettuata dal Titolare del trattamento, anche per il tramite dei Designati per specifici compiti e funzioni o del Referente aziendale in materia di protezione dei dati personali, tenuto conto:

- delle risultanze delle analisi dei rischi;
- delle evoluzioni organizzative interne;
- delle modifiche normative applicabili.

27.4 Le attività di verifica possono essere svolte mediante schede di revisione, checklists o piani di audit e danno luogo alla redazione di appositi report conservati agli atti.

27.5 Gli esiti delle verifiche possono comportare l'individuazione di eventuali non conformità e la definizione di misure correttive o di miglioramento.

25.6 I controlli possono essere svolti anche da soggetti esterni incaricati o dal Responsabile della protezione dei dati personali, nell'ambito delle funzioni di sorveglianza previste dall'art. 39 GDPR.

28. Allegati

28.1 Al presente modello organizzativo sono allegate le seguenti policy e procedure specifiche, che costituiscono parte integrante del sistema di gestione della protezione dei dati personali dell'Ente:

- procedura per l'inquadramento del ruolo privacy dei fornitori;
- procedura per la gestione delle richieste di esercizio dei diritti da parte degli interessati;
- policy di utilizzo consapevole degli strumenti informatici, della posta elettronica e della rete Internet;

- policy relativa alla conservazione e allo scarto dei documenti contenenti dati personali;
- procedura per la gestione degli incidenti di sicurezza e delle violazioni di dati personali;
- policy per la gestione degli account istituzionali e la continuità operativa dei servizi digitali.

28.2 L'Ente può adottare ulteriori policy e procedure operative, anche settoriali, finalizzate a garantire un livello adeguato di protezione dei dati personali. Tali misure, ancorché non espressamente elencate nel presente modello organizzativo, costituiscono parte integrante del sistema di gestione della protezione dei dati personali e sono aggiornate in relazione all'evoluzione del quadro normativo e organizzativo di riferimento.

29. Revisione e aggiornamento

29.1 Il presente documento è soggetto a revisione periodica o ad aggiornamento in caso di mutamenti normativi, organizzativi o tecnologici rilevanti.

30. Disposizioni finali

30.1 Il presente documento è reso disponibile ai soggetti interessati secondo le modalità ritenute più idonee dall'Ente.