



Regolamento

Attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

INDICE

Definizioni	3
Art. 1 – Oggetto	5
Art. 2 - Titolare del trattamento	5
Art. 3 - Finalità del trattamento	7
Art. 4 - Delegato al Trattamento	7
Art. 5 - Responsabile della protezione dati	10
Art. 6 - Sicurezza del trattamento	12
Art. 7 - Registro delle attività di trattamento	14
Art. 8 - Registro delle categorie di attività trattate	15
Art. 9 - Valutazione d'impatto sulla protezione dei dati	15
Art. 10 - Violazione dei dati personali	19
Art. 11 – Rinvio	20

Allegati

A) fac simile schema di registro attività di trattamento

B) fac simile schema di registro categorie attività di trattamento

C) fac simile schema di registro unico di trattamento

DEFINIZIONI

Ai fini del presente Regolamento, si intende per:

- a) **Titolare del trattamento:** l'autorità pubblica (il Comune o altro ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.
- b) **Delegato al trattamento/ Responsabile del trattamento:** rispettivamente il Dirigente dell'Ente (o Responsabile P.O. delegata) / il soggetto (esterno all'Ente) pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.
- c) **Sub-Delegato al trattamento (Referente):** il soggetto della struttura organizzativa del Comune, individuato da un Delegato al trattamento, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento.
- d) **Incaricato:** qualunque persona fisica che agisca sotto l'Autorità del Titolare o del Delegato o del Sub - Delegato (elabora o utilizza materialmente i dati personali).
- e) **Responsabile per la protezione dati – RPD:** il dipendente della struttura organizzativa del Comune, il professionista privato o impresa esterna, incaricati dal Titolare di svolgere i compiti di cui alla Sezione 4 “Responsabile della protezione dei dati” (articoli dal 37 al 39) del Regolamento UE 2016/679.
- f) **Registri delle attività di trattamento:** elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Delegato al trattamento secondo le rispettive competenze.
- g) **DPIA - Data Protection Impact Assessment” - “Valutazione d’impatto sulla protezione dei dati:** è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, di cui alla Sezione 3 “Valutazione d’impatto sulla protezione dei dati e consultazione preventiva” (articoli 35 e 36) del Regolamento UE 2016/679.
- h) **Garante Privacy:** il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente
- i) **RPROC:** Responsabile del procedimento (L.240/1990 e s.m.i.)
- l) **RGPD:** Regolamento UE 2016/679.

Ai fini dei registri allegati, si intende per:

Categorie di trattamento: Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

Categorie di dati personali: Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale; dati inerenti lo stile di vita; situazione economica, finanziaria, patrimoniale, fiscale; dati di connessione: indirizzo IP, login, altro; dati di localizzazione: ubicazione, GPS, GSM, altro.

Finalità del trattamento: Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune; Adempimento di un obbligo legale al quale è soggetto il Comune; Esecuzione di un contratto con i soggetti interessati; Altre specifiche e diverse finalità.

Misure tecniche ed organizzative: Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.

Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso; Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso; Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Categorie particolari di dati personali (art. 9 Regolamento UE 2016/679): Dati inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale, dati genetici e biometrici, dati relativi a condanne penali (Riferimento: "Dati sensibili" Codice Privacy D.Lgs. 196/2003)

Categorie interessati: Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

Categorie destinatari: Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.

Art. 1

Oggetto

1. Il presente Regolamento ha per oggetto misure procedurali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune della Spezia.

Art.2

Titolare del trattamento

1. Il Comune della Spezia è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare") che può delegare le relative funzioni a Dirigente o Responsabile P.O. delegata in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

- a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
- b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9. Questa valutazione può non essere realizzata per i trattamenti già in essere al 24 maggio 2018, purché questi siano previsti da norme o Regolamenti e vengano effettuati in base alle indicazioni del Garante Privacy.

6. Il Titolare, inoltre, provvede a:

- a) designare i Delegati al Trattamento, nelle persone dei Dirigenti delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;
- b) nominare il Responsabile della protezione dei dati;
- c) nominare quale Responsabile del Trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;
- d) predisporre l'elenco dei Delegati al Trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Delegati al Trattamento.

Art.3

Finalità del trattamento

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

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

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto con soggetti interessati;

d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento;

e) per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

Art.4

Delegato al Trattamento

1. Ciascun Dirigente (o Responsabile P.O. delegata dallo stesso), è nominato Delegato al Trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Delegato al Trattamento deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD. Pertanto il Dirigente (o Responsabile P.O. delegata), assicura, anche tramite i RPROC da lui designati, che:

a. Siano applicati i principi di cui all'art. 5 (RGPD) ed in particolare sia individuato il periodo di conservazione;

b. Sia correttamente individuata la liceità del trattamento di cui all'art. 6 (RGPD);

c. Sia assicurato l'effettivo esercizio dei diritti dell'interessato di cui agli artt. da 13 a 22 (RGPD), in collaborazione con il Responsabile dell'URP e dei Sistemi informativi;

- d. Sia assicurato il costante aggiornamento del Registro dei trattamenti di cui all'art. 30 (RGPD);
- e. Sia assicurata un'effettiva protezione dei dati con riferimento agli art. 25, 32, (RGPD) in collaborazione con gli altri uffici (Sistemi Informativi, Segreteria Generale/Affari Generali, Polizia Locale)
- f. Sia assicurata la liceità di eventuali comunicazioni e trasferimenti
- g. Il RPD sia informato delle più significative decisioni

Nelle procedure operative occorre venga distinta la figura del Delegato al Trattamento da quella dell'Amministratore di sistema (Responsabile del settore informatica, in qualità di referente informatico designato), poiché il primo deve individuare la liceità del trattamento, stabilire il periodo di conservazione dei dati, predisporre l'informativa, applicare il principio di minimizzazione del trattamento, individuare i rischi del trattamento, individuare le misure organizzative di protezione. L'Amministratore di sistema (Responsabile del settore informatica, in qualità di referente informatico designato), deve invece supportare tecnicamente il Delegato al Trattamento, predisponendo le misure tecniche di protezione (pseudomizzazione, cifratura, ...) in riferimento agli standard (misure minime di sicurezza Agenzia per l'Italia Digitale, ecc..).

2. I dipendenti del Comune, incaricati del trattamento, sono designati, di norma, mediante decreto di incarico del Dirigente di riferimento, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

Tale disciplina può essere contenuta anche in apposita procedura organizzativa.

3. Il Responsabile del procedimento (RPROC) può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di Responsabili del Trattamento, forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabile del Trattamento e le modalità di trattamento.

4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del Trattamento (esterno) devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali

oppure dalla Commissione europea. Il RPROC ha il compito di redigerli in modo da assicurare un'effettiva protezione dei dati e dei diritti dell'interessato.

5. E' consentita la nomina di sub-Delegati al Trattamento da parte di ciascun Delegato al Trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Delegato primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Delegato attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Il Delegato risponde, anche dinanzi al Titolare, dell'operato del sub-delegato anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-delegato.

6. Il Delegato al Trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

7. Il RPROC assicura che il Delegato al Trattamento dei dati provveda, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ossia:

- la tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- l'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- la sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- informare il Titolare (o figura designata tramite procedura interna), senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

In aggiunta agli obblighi sopra previsti per il Delegato al Trattamento (interno all'Ente), per il Responsabile del Trattamento "esterno" (esempio: i fornitori dell'Ente), si aggiunge la designazione del RPD qualora richiesta, poiché è una possibilità espressamente prevista per questa figura.

Art.5

Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con “RPD”) del Comune della Spezia occorre venga designato da parte dell’organo competente ed il relativo nominativo pubblicato sulla sezione web “Amministrazione Trasparente” del sito istituzionale dell’Ente e comunicato al Garante Privacy.

Il RPD è incaricato dei seguenti compiti:

- a) informare e fornire consulenza al Titolare ed al Delegato al Trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Delegato al Trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
- b) sorvegliare l’osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Delegato al Trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l’analisi e la verifica dei trattamenti in termini di loro conformità, l’attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Delegato al Trattamento;
- c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Delegato al Trattamento;
- d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
- e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all’art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Delegato al Trattamento al Garante;
- f) la tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o il Delegato al Trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

2. Il Titolare ed il Delegato al Trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:

- a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Delegato al Trattamento.

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Delegato al Trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il Titolare ed il Delegato al Trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;
- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e personale tramite la costituzione di un gruppo di lavoro (preferibilmente intersettoriale) coordinato dal RPD e per suo conto dal Referente Privacy in staff al Segretario Generale;
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il RPD non può essere rimosso o penalizzato dal Titolare e dal Delegato al Trattamento per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Delegato al Trattamento.

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Delegato al Trattamento.

Art.6

Sicurezza del trattamento

1. Il Comune della Spezia e ciascun Delegato al Trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i

diritti e le libertà delle persone fisiche. Ciascun RPROC, con il sostegno del proprio Dirigente/PO delegata assicura che il trattamento avvenga secondo le direttive riguardanti la gestione del rischio, approvate dal Sindaco o della Giunta Comunale. Il RPROC collabora con gli altri uffici per raggiungere gli obiettivi di sicurezza volti a neutralizzare il rischio stesso.

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

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Delegato al Trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) in collaborazione con i Sistemi Informativi;
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico in collaborazione con il Dirigente che ha la responsabilità della sicurezza degli immobili.

In riferimento all'ultimo punto, nelle procedure operative occorre venga distinta la responsabilità della sicurezza degli immobili da quella fisica (presidio delle sedi, sistemi di allarme...) e le relative forme di collaborazione.

4. Occorre in particolare, che venga creato un sistema di procedure operative interne (IOP) che definisca come applicare ciascun articolo del presente Regolamento ed i compiti del personale a ciò deputato. Al riguardo viene individuato il Referente Privacy in Staff al Segretario Generale con il compito di definire tali procedure, in collaborazione con le strutture dell'Ente, e di aggiornarle.

5. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato o mediante la verifica dell'applicazione del Sistema di procedure operative interne, tenuto e aggiornato dal Referente sopra indicato.

5. Il Comune della Spezia e ciascun Delegato al Trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure/istruzioni operative, a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare, dei Delegati al Trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione “privacy” eventualmente già presente.

7. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art.7

Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

- a) il nome ed i dati di contatto del Comune, del Sindaco e/o del suo Delegato ai sensi del precedente art. 2, eventualmente del Contitolare del trattamento, del RPD;
- b) le finalità del trattamento;
- c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa del Comune in forma telematica, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

4. Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo art. 8, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema allegato C al presente Regolamento. In tal caso, il Titolare delega la sua tenuta al Delegato al Trattamento di cui al precedente art. 4 o, comunque, ad un solo delegato al Trattamento, ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Delegato al Trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art.8

Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Delegato di cui al precedente art. 4, reca le seguenti informazioni:

- a) il nome ed i dati di contatto del Delegato al Trattamento e del RPD;
- b) le categorie di trattamenti effettuati da ciascun sub – delegato/RPROC/incaricato: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
- c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il registro è tenuto, tramite una specifica applicazione, dal sub-delegato o RPROC di ciascun trattamento.

Art.9

Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

- a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
- b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
- c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
- d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
- e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
- f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
- g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
- h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare

un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Il Delegato al Trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante

Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i Responsabili del Trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

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

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di

compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

11. E' opportuno procedere, nel tempo, alla pubblicazione sul sito istituzionale dell'Ente, in apposita sezione, di una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

12. Il RPROC di ciascun trattamento è responsabile del rispetto di quanto previsto nel presente articolo.

Art. 10

Violazione dei dati personali

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

2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Delegato al Trattamento (se esterno, il Responsabile del Trattamento), è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;

- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

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

5. La notifica deve avere il contenuto minimo previsto dall’art. 33 RGPD, ed anche la comunicazione all’interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

7. Il Segretario Generale (o un suo delegato) è tenuto a definire, in collaborazione con i Responsabili delle altre strutture, una procedura per la gestione dei flussi interni e per la gestione degli eventi che possano potenzialmente costituire una violazione, in modo da assicurare il pieno rispetto del RGPD.

Art.11

Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

(segue: allegati)

