Comune di Potenza

Regolamento sulla Protezione dei Dati Personali, in attuazione del Regolamento UE 2016/679.

Indice

CAPO I PRINCIPI

Art. 1 - Definizioni....4
Art. 2 - Oggetto ……..10
Art. 3 - Finalità del Regolamento....11
Art. 4 - Finalità del Trattamento 12

CAPO II SOGGETTI DEL TRATTAMENTO DEI DATI PERSONALI

Art. 5 - Titolare del Trattamento....13
Art.6 - Competenze e organizzazione....14
Art. 7 - Dirigenti e personale autorizzato al trattamento....15
Art. 8 - Amministratore di sistema....17
Art. 9 - Contitolarità del trattamento 18
Art. 10 - Responsabili del Trattamento 18
Art. 11- Il Responsabile della protezione dei dati (DPO/RPD)....19

CAPO III TRATTAMENTO DEI DATI PERSONALI

Art. 12 - Attività amministrativa....21
Art.13 - Trattamento dei dati particolari e dei dati relativi a condanne penali e reati....22
Art. 14 - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi 23
Art. 15 - Pubblicazione web per obblighi di trasparenza....24
Art. 16 - Pertinenza delle informazioni contenenti dati personali....25
Art. 17 - Registro del trattamento....26
Art. 18 - Fascicolo personale dipendenti e amministratori....27
Art. 19 - Sensibilizzazione e formazione del personale....27

CAPO IV ACCESSO AI DATI PERSONALI

Art. 20 - Trattamento interno dei dati personali....28
Art. 21 - Utilizzo dei dati da parte dei Componenti gli Organi di Governo e di Controllo Interno 28
Art. 22 - Trasmissione interconnessione e scambio di dati con altri soggetti....28
Art. 23 - Accesso ai dati personali da parte di soggetti privati....29

CAPO V DIRITTI DELL'INTERESSATO

Art. 24 - Diritti dell'interessato.....30
Art. 25 - Modalità di esercizio dei diritti dell'interessato.....31
Art. 26 - Indagini difensive.....32
Art. 27 - Obbligo di informativa.....33
Art. 28 - Modulistica e procedure 33

CAPO VI MISURE DI SICUREZZA

Art. 29 - Piano di Protezione dei dati personali e gestione del rischio di violazione.....34
Art. 30 - Misure di sicurezza……..…… 34
Art. 31 - Valutazione di impatto sulla protezione dei dati personali (DPIA).....35
Art. 32 - Pubblicazione sintesi della valutazione d'impatto (D.P.I.A.).....37
Art. 33 - Sistema e politiche di audit…… … 38
Art. 34 - Procedimento audit…….38

CAPO VII DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

Art. 35 - Definizione di violazioni dei dati personali.....39
Art. 36 - Notifica violazioni dei dati personali.....39
Art. 37 - Comunicazione di una violazione dei dati personali agli interessati.....40

CAPO VIII MEZZI DI TUTELA E RESPONSABILITA'

Art. 38 - Soggetti responsabili ed azione risarcitoria.....40
Art. 39 - Reclamo.....41
Art. 40 - Trattamento illecito dei dati.....41
Art. 41 - Falsità nelle dichiarazioni e notificazioni al Garante della privacy.....41
Art. 42 - Omessa predisposizione di misure di sicurezza.....41

CAPO IX ENTRATA IN VIGORE E DISPOSIZIONI FINALI

Art. 43 - Entrata in vigore del regolamento.....42
Art. 44 - Disposizioni finali.....42

CAPO I PRINCIPI

Art. 1 - Definizioni

1. Ai fini del presente regolamento si intende per:

1) "**accountability**": *letteralmente "rendere conto", ovvero, il Titolare del trattamento si deve responsabilizzare autonomamente nella gestione ed organizzazione della Privacy. Il principio nasce nella legislazione europea e statunitense ed è inteso come la responsabilità dell'amministrazione ha verso chi l'ha scelta e s fonda su: trasparenza intesa come informazioni dell'attività di governo; partecipazione di chiunque al miglioramento delle politiche pubbliche e collaborazione intesa come efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo*.

*2) "**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.*

*3) "**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.;*

*4) "**identificazione/identificabilità**", Identificata/identificabile è una condizione della persona, rispettivamente effettiva (identificata) o possibile (identificabile)*

*5) "**dato pluripesonale**", Dato che può essere collegato a più soggetti, dunque presentare una pluralità di interessati*

*6) "**dati particolari**", si tratta dei dati c.d. ex* "sensibili"*, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute, alla vita o all'orientamento sessuale, nonché i dati genetici e i dati biometrici;*

*7) **"i dati relativi a condanne penali e reati"**: si tratta dei dati c.d.* "giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la*

liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Inoltre, i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

8) **"*titolare del trattamento*":** *La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membr.;*

*9) "**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, come regolato dall'art. 28 del Regolamento UE 679/2016.*

*10) "**autorizzati**", le persone fisiche a cui sono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali attribuiti dal titolare del trattamento o dal responsabile del trattamento, sotto la propria responsabilità e nell'abito del proprio assetto organizzativo, espressamente designate, che operano sotto la loro autorità*

*11) "**interessato**", La persona fisica identificata o identificabile cui si riferiscono i dati personali.*

*12) "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*

*13) "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*

*14) "**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*

*15 "**Informazione anonima**", Informazione che non riguarda una persona fisica identificata o identificabile*

*16 "**diritto all'informativa**", diritto di una persona di comprendere e prevedere il flusso di circolazione dei propri dati, le finalità del trattamento, i soggetti del trattamento per arrivare ad una ragionevole autodeterminazione*

*17) "**diritto di accesso**", Il diritto di accesso è una declinazione del diritto di informativa, diritto conoscitivo che non avviene su iniziativa del titolare del trattamento come nel caso*

precedente ma, su iniziativa dell'interessato

*18) "**diritto di limitazione**", Il diritto di limitazione del trattamento è volto ad assicurare pretese dell'interessato e verifiche limitando il trattamento in corso alla sola conservazione.*

*19) "**diritto di opposizione**", diritto che permette all'interessato di impedire un trattamento che non ha preventivamente autorizzato (opt-in) ma, che può essere iniziato senza la sua preventiva volontà di farne parte come interessato (opt-out).*

*20) "**diritto di portabilità**", diritto di creare una copia dei dati personali in possesso del titolare in un formato comune e leggibile da un calcolatore ove tecnicamente fattibile*

*21) "**diritto di rettifica e integrazione**", diritto di vedere i propri dati accurati e ed esatti*

*22) "**diritto di cancellazione e all'oblio**", permette all'interessato di rimuovere informazioni personali che lo riguardano dalla pubblica circolazione ove il loro rilievo di pubblico interesse sia ridotto, in funzione del tempo trascorso e per altre ragioni*

*23) "**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*

*24) **"autorità di controllo"**: L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.*

*25) **"autorità di controllo interessata"**: Un'autorità di controllo interessata dal trattamento di dati personali i n quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un r eclamo è stato proposto a tale autorità di controllo.*

*26) "**data protection by design**": Il principio secondo cui sono tutelati i diritti degli interessati sin dalla progettazione di qualsiasi attività anche mediante l'utilizzo di misure tecniche e organizzative volte alla protezione dei dati personali e comunque secondo quanto definito dall'art.25 paragrafo 1 del Regolamento UE 679/2016.*

*27) "**data protection by default**": Il principio secondo cui l'adozione di misure tecniche e organizzative adeguate deve realizzarsi per impostazione predefinita e comunque secondo quanto definito dall'art.25 paragrafo 2 del Regolamento UE 679/2016.*

*28) "**DPIA (Data Protection Impact Assessment)":** Attività di valutazione di impatto dei rischi di trattamento dei dati personali prevista dall'Articolo 35 Regolamento UE 679/2016.*

*29) "**GDPR**": 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

*30) "**ponderazione del rischio**": processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio e/o la sua espressione quantitativa sia accettabile o tollerabile.*

*31) "**processo**": Insieme di attività tra loro correlate o interagenti le quali trasformano input in output.*

*32) "**profilazione**": Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.*

*33) "**pseudonimizzazione**": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;*

*34) "**rappresentante**": La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del Regolamento UE 679/2016.*

*35) "**sistema di Gestione dei Dati Personali (GDP**)": Parte del generale sistema di gestione che stabilisce, implementa, attua, monitora, rivede, mantiene, migliora i processi di conformità al trattamento dei dati personali.*

*36) "**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.*

*37) "**valutazioni**": processo complessivo di identificazione del rischio, analisi del rischio e ponderazione del rischio.*

*38) "***audit privacy***": valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Reg. UE n. 679/2016.*

*39) "**chiamata**", la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;*

*40) "**reti di comunicazione elettronica**", i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;*

*41) "**rete pubblica di comunicazioni**", una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;*

*42) "**servizio di comunicazione elettronica**", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;*

*43) "**contraente**", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;*

*44) "**utente**", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;*

*45) "**dati relativi al traffico**", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;*

*46) "**dati relativi all'ubicazione**", ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;*

47) "***dati genetici***": *i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*

48) "***dati biometrici***": *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;*

49) "***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;*

*50) "**servizio a valore aggiunto**", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;*

*51) "**posta elettronica**", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.*

*52) "**misure di sicurezza**", Misure tecniche ed organizzative adeguate idonee e adeguate a garantire la sicurezza di ogni trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche.*

*53) "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;*

*54) "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;*

*55) "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;*

*56) "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;*

*57) "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;*

*58) "**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;*

*59) "**violazione di dati personali (data breach)**": la violazione della 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;

*60) "**scopi storici**", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;*

*61)"**scopi statistici**", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;*

*62) "**scopi scientifici**", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.*

63) "***obiezione pertinente e motivata***": un'obiezione rispetto ad un provvedimento o ad un'attività di questa amministrazione sul fatto che vi sia o meno una violazione del presente regolamento, che dimostra chiaramente la rilevanza dei rischi riguardo ai diritti e alle libertà fondamentali degli interessati.

Art. 2 - Oggetto

1. Il presente regolamento disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, la gestione delle misure tecniche e organizzative individuate dal Comune di Potenza, in relazione allo svolgimento delle proprie finalità istituzionali con riguardo ai trattamenti dei dati personali e particolari, nonché alla libera circolazione di tali dati, in attuazione a:

- Linee guida e raccomandazioni del Garante;
- Regolamento UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito GDPR);
- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (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 e che abroga la direttiva 95/46/CE;
- D.lgs. 10/08/2018, n. 101 di adeguamento della normativa interna al GDPR che ha modificato il codice della protezione dei dati personali d.lgs. 196/2003;
- Dichiarazioni del gruppo di lavoro WP29 sulla protezione dei dati.
- Linee-guida sui responsabili della protezione dei dati (RPD) – WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" – Adottate dall'ex WP29 il 13 dicembre 2016;

- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento – adottate dal ex WP29 il 13 dicembre 2016;

- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 – WP29 il 4 aprile 2017;

- Linee guida elaborate dal ex WP29 in materia di applicazione e definizione delle sanzioni amministrative –adottate dal l'ex WP29 il 3 ottobre 2017;

- Linee guida elaborate dall'ex WP29 in materia di processi decisionali automatizzati e prolazione – dall'ex WP29 il 6 febbraio 2018;

- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) – adottate dall'ex WP29 il 6 febbraio 2018;

- Parere dell'ex WP29 sulla limitazione della finalità – 13/EN WP 203;

- Normativa in materia di diritto di accesso documentale, accesso civico e accesso generalizzato.

Art. 3 – Finalità del Regolamento

1. Il Comune di Potenza, in qualità di Titolare del trattamento dei dati personali (di seguito Titolare), nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità sanciti dalla legislazione vigente, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto degli individui all'autodeterminazione informata come definito dalla convenzione europea 108/1981.

2. In adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa, la finalità del presente regolamento è di favorire la trasmissione di dati e documenti, contenuti nelle banche dati e gli archivi in dotazione, con gli enti territoriali, gli enti pubblici, i gestori e gli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea.

3. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità.

4. Ai fini del presente regolamento, per finalità istituzionali del Comune di Potenza si intendono le funzioni ad esso attribuite dalle leggi, dallo statuto e dai regolamenti, anche svolte per mezzo di intese, accordi, convenzioni.

Art. 4 – Finalità del Trattamento

1. Il sistema di gestione dei dati personali deve essere determinato in modo coerente agli obiettivi istituzionali. È necessario determinare i confini e l'applicabilità del sistema di gestione dei dati personali al fine di stabilirne il campo di applicazione.

2. È necessario determinare le finalità dei trattamenti di dati personali coerentemente con gli obbiettivi istituzionali e di gestione del sistema informativo.

3. I trattamenti effettuati da questa organizzazione devono avvenire in maniera lecita e corretta, informando i soggetti interessati circa la raccolta, l'utilizzo e la consultazione dei loro dati o ulteriori tipologie di trattamenti effettuate, precisando in che misura essi sono o saranno trattati al fine di garantire la trasparenza.

4. Per ogni finalità dei trattamenti effettuati da questa organizzazione, deve essere individuata la base giuridica che legittima il trattamento, prima dell'inizio del trattamento.

5. La determinazione delle finalità ex ante è un obbligo per l'organizzazione e una garanzia per l'interessato

6. Questo Ente tratta dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri in relazione a funzioni e compiti attribuiti o delegati, nonché tutte quelle inerenti all'attività amministrativa, per necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.

7. Nel caso in cui un trattamento di dati personali è necessario per l'esecuzione di compito di interesse pubblico o connesso all'esercizio di pubblici poteri è necessario individuare la base di legittimazione in norma europea o nazionale, o, nei casi previsti dalla legge, di regolamento. In questo caso la norma europea o nazionale deve determinare anche le finalità del trattamento, infatti in questo caso rileva sussistenza di un rapporto necessario tra finalità del trattamento ed esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

8. I trattamenti delle categorie particolari (ex sensibili) e giudiziari, necessari per motivi di interesse pubblico rilevante sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

9. Per finalità diverse da quelle dei cui ai commi precedenti, purché l'interessato abbia espresso il proprio consenso.

CAPO II SOGGETTI DEL TRATTAMENTO DEI DATI PERSONALI

Art. 5 – Titolare del Trattamento

1. Il Comune di Potenza, rappresentato legalmente dal Sindaco pro-tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto le 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 GDPR, 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 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione generale dell'Ente (Documento Unico di Programmazione -DUP) e negli altri documenti di programmazione e pianificazione (PEG, Piano degli obiettivi/della *Performance*), 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.
5. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.

6. Nel caso in cui un tipo di trattamento, anche per 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 (*Data Protection Impact Analysis,* di seguito indicata con l'acronimo "DPIA") , ai sensi dell'art. 35 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 31(DPIA).

7. Il Titolare, sulla base del proprio ordinamento, provvede a individuare:
   a) gli autorizzati al trattamento dei dati personali, ciascuno in relazione ai procedimenti amministrativi singolarmente assegnati;
   b) il Responsabile della Protezione dei Dati (*Data Protection Officer* -DPO/RDP);

c) i Responsabili del trattamento, ovvero soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione Comunale, in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge.

8. Il Titolare, prima del trattamento dei dati personali, valuta i casi di contitolarità e stipula i relativi accordi, secondo l'art.26 del GDPR.

Art.6 - Competenze e organizzazione

1. Al Segretario Generale e ai suoi Uffici è affidata la competenza in materia di Privacy. Con il supporto del Referente interno della Privacy, cura le attività in materia, al fine di fornire il necessario apporto tecnico-amministrativo al Titolare e al DPO/RPD.
2. Il Segretario Generale provvede alla predisposizione delle proposte di provvedimenti da adottarsi in materia, da parte del Sindaco, della Giunta e del Consiglio Comunale.
3. Il Segretario Generale istituisce lo Staff Privacy, coordinato dal DPO/RPD e composto dal Referente interno della privacy dell'Ente, dipendente comunale di categoria D, nominato dal Segretario Generale, competente in materia di *governance* e gestione della protezione dei dati personali, e dai "referenti privacy", designati dai Dirigenti.
4. Allo Staff sono affidati i seguenti compiti:

a) collaborare con i dirigenti, per l'elaborazione della pianificazione strategica del sistema di sicurezza e di protezione dei dati personali, sensibili e giudiziari attraverso l'elaborazione di un Piano per la sicurezza/protezione, da sottoporre all'approvazione del titolare;

b) identificare contitolari, responsabili e sub responsabili di riferimento della struttura organizzativa di competenza, e coadiuvare o dirigenti nella definizione di accordi interni e i contratti per il trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari e ai responsabili (Aggiornando registro delle evidenze);

c) coadiuvare i dirigenti nella predisposizione degli atti per identificare e designare, per iscritto e in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, che operano sotto la diretta autorità del titolare, e attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati, per il conferimento di apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento;

d) coadiuvare gli uffici come punto di contatto con il DPO/RPD e il Responsabile interno privacy.

e) coadiuvare i dirigenti nella ricognizione di tutti i trattamenti di dati personali, sensibili e giudiziari svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ufficio, da sottoporre all'approvazione del titolare;

f) coadiuvare i dirigenti ad effettuare l'analisi del rischio dei trattamenti, e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli interessati, da sottoporre all'approvazione del titolare;

g) coadiuvare i dirigenti effettuare prima di procedere al trattamento, quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in parti-

colare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali;

h) in caso di violazione dei dati personali, collaborare con il titolare, il DPO/RPD per notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;

i) coadiuvare i dirigenti affinchè il DPO/RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;

j) coadiuvare i dirigenti a sostenere il DPO/RPD nell'esecuzione dei compiti fornendogli le informazioni e documenti necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;

k) collaborare con i dirigenti designati e delegati e con la Segreteria Generale per l'elaborazione e l'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di *data breach*, da sottoporre all'approvazione del titolare;

l) coadiuvare i dirigenti nel documentare tutte le attività e adempimenti delegati e, in ogni caso, a tracciare documentalmente l'intero processo di gestione dei rischi e del sistema di sicurezza e protezione;

m) coadiuvare i dirigenti ad attuare la formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto;

n) coadiuvare i dirigenti a promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;

o) coadiuvare i dirigenti ad effettuare ogni ulteriore attività, non espressamente indicata in precedenza e necessaria per la integrale attuazione del GDPR e della normativa interna di adeguamento;

p) svolgere ogni altro compito assegnato dal DPO/RPD.

Art. 7 – Dirigenti e personale autorizzato al trattamento

1. Il Titolare conferisce i sotto indicati compiti, funzioni e i correlati poteri, mediante apposito provvedimento di designazione da adottarsi secondo il proprio ordinamento, ai Dirigenti e a tutti i dipendenti dell'organizzazione.
2. Nel suddetto provvedimento, il Titolare deve informare ciascun dipendente, delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento.
3. I Compiti, le funzioni e i poteri assegnati ai dirigenti:
   a) trattare i dati personali solo su istruzione del titolare del trattamento;
   b) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
   c) adottare il tempestivo ed integrale rispetto dei doveri del titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR;
   d) osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal titolare;
   e) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale,

fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;

f) collaborare con il Titolare per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con l'amministratore di sistema e con le altre strutture competenti del titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;

g) curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del titolare per l'applicazione del Codice, del GDPR, e del presente Regolamento;

h) informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*") nelle modalità previste dal Capo VII del presente regolamento, 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;

i) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a disposizione. In particolare provvedere alla valutazione d'impatto sulla protezione dei dati personali, consultando il DPO/RPD come previsto dal'art. 35 del Regolamento UE 679/2016 e tenuto conto del provvedimento del Garante per la protezione dei dati personali [doc. web n. 9058979]

j) informare il Titolare, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

k) curare le previste comunicazioni e notificazioni al garante.

l) curare le informative di cui agli artt. 13 e 14 del GDPR da fornire agli interessati, predisponendo la necessaria modulistica o determinando altre forme idonee di informazione inerenti ai trattamenti di competenza della propria struttura organizzativa, facendo, in presenza di dati sensibili, espresso riferimento alla normativa che prevede gli obblighi o i compiti in base al quale è effettuato il trattamento. Al fine di rendere conforme la prassi di redazione delle informative, con l'allegato 1 a questo regolamento si approva uno schema di informativa tipo che dovrà essere utilizzato dagli autorizzati al trattamento e dai dirigenti dati e aggiornato in base alle ultime modifiche normative;

m) assistere il Titolare con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;

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

o) predisporre una relazione in merito all'avvenuta adozione, nell'ambito delle articolazioni organizzative di loro competenza, delle misure adottate a garanzia del trattamento dati e alle

conseguenti risultanze, da trasmettere alla Segreteria Generale - Referente interno Privacy, di cui al precedente art. 6, con periodicità annuale o su richiesta di quest'ultimo o dello Staff Privacy;

p) contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente regolamento, comprese le ispezioni, realizzate dal titolare o da un altro soggetto da questi incaricato;

q) curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza:
   • elenco dei contitolari, dei responsabili dei trattamenti, e degli autorizzati con i relativi punti di contatto;
   • elenco degli archivi/ banche;

r) garantire l'aggiornamento, almeno annuale, della ricognizione dei trattamenti;

s) fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (di seguito DPO) nell'esercizio delle sue funzioni;

t) garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa del titolare e all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;

u) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, GDPR e nel presente Regolamento.

4. Ciascun dirigente, nell'espletamento dei compiti, funzioni e poteri per i quali è stato designato, è delegato a designare:

   a) il personale assegnato quale autorizzato al trattamento dei dati personali, in relazione ai procedimenti amministrativi a cui è singolarmente preposto, come richiesto dal d.lgs. 101/2018 Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati), fornendo loro specifiche istruzioni;

   b) uno o più "incaricati privacy" per ciascuna direzione, con il compito di supportare gli autorizzati al trattamento dei dati personali, sia a livello informativo che operativo. Gli incaricati privacy sono componenti dello Staff Privacy, di cui all'art. 6

Art. 8 – Amministratore di sistema

1. Il Titolare individua i dipendenti assegnati al Servizio Informativo-Informatico dell'Ente, operanti sul sistema informatico di cui è dotata l'Amministrazione, quali Amministratori di Sistema.
2. La designazione di Amministratore di sistema deve avvenire previa valutazione dell'esperienza della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Ogni anno è necessario valutare le competenze degli amministratori di sistema mediante valutazioni ad hoc sulle competenze e abilità di questi.
3. L'Amministratore di sistema svolge attività, quali: il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware e propone al Titolare un documento di valutazione del rischio informatico.

4. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'Amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste; devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore a sei mesi.
5. L'Amministratore di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici, relativamente alle attribuzioni delle funzioni di Amministratore di sistema.

Art. 9 – Contitolarità del trattamento

1. Il GDPR disciplina con l'art. 26 l'ipotesi in cui Il trattamento dei dati personali può essere effettuato da uno o più titolari.
2. In situazioni di "contitolarità" del trattamento e cioè quando "due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento" è stipulato un accordo scritto con il quale si disciplinano le responsabilità, il rispetto degli obblighi previsti dal GDPR e i ruoli, con pubblicità dell'avvenuta stipula presso le sedi dei contitolari del trattamento.
3. Gli accordi di contitolarità dovranno indicare in maniera trasparente le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo deve prevedere espressamente la modalità con cui gli interessati possano far valer i proprio diritti o richiedere informazioni.
4. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
5. Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

Art. 10 – Responsabili del Trattamento

1. Il Titolare può prevedere l'esternalizzazione totale o parziale di un trattamento di dati personali mediante delega, concessione o contratto.
2. Questa fattispecie non implica alcuna deresponsabilizzazione per il Titolare che dovrà verificare la conformità normativa delle attività di trattamento esternalizzate.
3. Nel caso di esternalizzazione del trattamento di dati personali è necessario formalizzare, in forma scritta, gli obblighi delle parti preposte alle attività di trattamento, definendone modalità, condizioni, durata, natura e finalità, chiarendo, espressamente, il tipo di dati personali trattati, le categorie di interessati, nonché gli obblighi e i diritti del Titolare e del Responsabile del trattamento designato.

4. La designazione formale è necessaria sia nel caso in cui il Titolare affidi uno specifico trattamento a un Responsabile sia qualora un Responsabile del trattamento affidi a un altro responsabile del trattamento (sub-responsabile) l'esecuzione di specifiche attività di trattamento per conto del Titolare.
5. Gli accordi con il Responsabile del trattamento, obbligatoriamente in forma scritta e con atto vincolante, devono prevedere: l'obbligo di trattare i dati solo in conformità alle istruzioni ricevute dal Titolare; l'obbligo di garantire che le persone fisiche autorizzate alle attività di trattamento siano vincolate da obblighi di riservatezza, contrattualmente assunti o stabiliti per legge; l'obbligo di adottare le misure richieste ai sensi dell'art. 32 del GDPR, vale a dire le misure tecniche e organizzative a protezione dei dati ritenuti idonee a garantire un livello di sicurezza, adeguato al rischio insito nel trattamento; l'imposizione degli stessi obblighi verso l'eventuale sub-responsabile; l'obbligo di assistere il Titolare, mediante misure tecniche e organizzative adeguate, e nella misura in cui ciò sia possibile, nel dar seguito alle eventuali richieste degli interessati (accesso, rettifica, cancellazione, portabilità, opposizione); le attività di notificare di eventuali *data breach.*

Art. 11 – Il Responsabile della protezione dei dati (DPO/RPD)

1. Il Titolare si avvale obbligatoriamente di un Responsabile della protezione dei dati (DPO/RPD), in possesso di idonee qualità professionali. In particolare la conoscenza specialistica della normativa e delle prassi, in materia di protezione dei dati e la capacità tecnico-specialistica di assolvere i compiti di competenza.
2. Il Titolare non può procedere nella sua attività istituzionale, in assenza del DPO/RPD (art. 37 del GDPR).
3. Il DPO/RPD può essere un dipendente in posizione apicale oppure un incaricato con contratto di servizio, previo espletamento di procedura ad evidenza pubblica.
4. In caso di DPO/RPD designato con contratto di servizio, l'individuazione dello stesso avviene a seguito di determina di aggiudicazione ai sensi del D.Lgs. n. 50/2016.
5. La figura del DPO/RPD è incompatibile con chi determina le finalità o i mezzi del trattamento. In particolare, risultano con la stessa incompatibili:
    a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
    b) il Responsabile del trattamento;
    c) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
6. Sul sito istituzionale devono essere pubblicati i dati di contatto del DPO/RPD, da comunicarsi, altresì, al Garante della protezione dei dati personali.
7. Il DPO/RPD deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e gli vanno fornite le risorse necessarie per assolvere tali compiti, accedere ai dati personali, ai trattamenti e per mantenere la propria conoscenza specialistica.
8. Gli interessati possono contattare il DPO/RPD per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
9. Il DPO/RPD è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti. In conformità del diritto dell'Unione o degli Stati membri deve svolgere almeno le seguenti funzioni:

a) informare e fornire consulenza al Sindaco, ai Dirigenti, agli organi collegiali e di Indirizzo e Controllo e a tutti gli uffici in merito agli obblighi derivanti dal presente regolamento nonché dalla normativa nazionale e comunitaria;
b) sorvegliare l'osservanza del presente regolamento nonché della normativa nazionale e comunitaria da parte del Titolare e del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con l'Autorità garante per la protezione dei dati personali e fungere da punto di contatto per questioni connesse al trattamento dei dati personali

10. Il DPO/RPD è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione con onere di comunicazione di detto adempimento al Titolare.

11. Il Titolare ed il Responsabile del trattamento assicurano che il DPO/RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

a) il DPO/RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
b) il DPO/RPD deve ricevere tempestivamente tramite posta elettronica, dal Titolare e dal Responsabile del trattamento dati, tutte le informazioni pertinenti le decisioni che impattano sulla protezione dei dati, in modo da prestare idonea consulenza;
c) il DPO/RPD esprime, sulle decisioni che impattano sulla protezione dei dati, un parere che è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO/RPD, è necessario motivare specificamente tale decisione;
d) il DPO/RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o altro incidente (*Data Breach*): all'uopo, con proprio parere, indica i provvedimenti da adottarsi per porre rimedio o per prevenire il ripetersi di tali violazioni.

12. Nello svolgimento dei compiti affidatigli il DPO/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 DPO/RPD:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati avvalendosi della collaborazione dei Responsabili del trattamento dati interessati nell'area di mappatura;
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 Responsabile del trattamento.

13. Il Titolare ed il Responsabile del trattamento forniscono al DPO/RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali e ai trattamenti. In particolare, è assicurato al DPO/RPD:

    a) il tempo sufficiente per l'espletamento dei compiti affidati;

    b) un supporto adeguato in termini di risorse finanziarie, strumentali (sede, attrezzature) e, di personale compatibilmente con la capacità di bilancio e la dimensione organizzativa;

    c) l'apporto dello Staff Privacy di cui all'art.6;

    d) la comunicazione ufficiale dell'avvenuta nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;

    e) l'accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

14. Il DPO/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 la normativa in materia di protezione dei dati. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO/RPD riferisce direttamente al Titolare.

15. Il DPO/RPD è tenuto a manifestare il proprio dissenso su decisioni/provvedimenti/comportamenti incompatibili con il GDPR, adottati o tenuti dai componenti degli organi di governo e di controllo nonché degli organi di gestione e dei dipendenti, ogni qual volta ne venga a conoscenza, dandone comunicazione al Titolare, al Responsabile del trattamento interessato dai rilievi e, ove necessario, al Gestore informatico. I Responsabili del trattamento qualora non condividano i rilievi formulati dal DPO/ RPD, comunicano a quest'ultimo e al Titolare le proprie osservazioni. Il DPO/RPD dirama le direttive utili a prevenire il ripetersi delle violazioni rilevate.

CAPO III TRATTAMENTO DEI DATI PERSONALI

Art. 12 - Attività amministrativa

1. L'attività amministrativa del Comune di Potenza si svolge, principalmente, con l'emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.

2. Per l'attività amministrativa di cui al comma precedente sono rigorosamente rispettate le regole comportamentali (**Allegato 1**), da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Ente.

3. Per l'attività informatica di cui al comma precedente sono rigorosamente rispettate le norme di cui al codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive

modificazioni e le istruzioni operative all'utilizzo dei sistemi informatici allegato a questo regolamento (**Allegato 2**)

4. La gestione dei documenti informatici contenenti dati personali è soggetta alla specifica disciplina prevista dal GDPR 679/2016 e del D.lgs. n. 196/2003 e al regolamento di gestione dei documenti informatici.

5. La sicurezza dei dati personali contenuti nei documenti di cui al precedente comma 3 è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche idonee al trattamento dei dati personali e sensibili come pseudonimizzazione, criptazione dei dati.

Art.13 - Trattamento dei dati particolari e dei dati relativi a condanne penali e reati

1. Il Titolare conforma il trattamento di tali dati secondo modalità volte a prevenire violazioni dei diritti delle libertà fondamentali e della dignità dell'interessato.

2. I trattamenti delle categorie particolari di dati personali e dei dati relativi a condanne penali e reati di cui agli art 9 e 10 del GDPR, necessari per motivi di interesse pubblico rilevante ai sensi della lettera g), paragrafo 2, del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, da regolamenti che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. Il Titolare tratta i dati particolari che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici, dati relativi alla salute, alla vita sessuale:

   a) per motivi di interesse pubblico rilevante quando questo è previsto da una norma di legge o di regolamento;

   b) per un interesse vitale dell'interessato o di altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

   c) se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche;

   d) per diritti dell'interessato in materia di diritto del lavoro, sicurezza sociale e protezione sociale, in base a norma di legge o contratto collettivo;

   e) se il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

   f) se il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o

storica o a fini statistici ed è proporzionato alla finalità perseguita.

4. In tutti gli altri casi è fatto divieto assoluto di trattare tali dati (art. 9 paragrafo 1 GDPR).

5. Il Titolare tratta i dati relativi a condanne penali e reati: il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento come previsto dal d. lgs. 101/2018 art 2-octies comma 2.

6. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

7. I dati particolari e i dati relativi a condanne penali e a reati sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, soprattutto nel caso in cui la raccolta non avvenga presso l'interessato.

8. I dati particolari e i dati relativi a condanne penali e a reati non indispensabili, dei quali il Titolare, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato, comunque, non a richiesta del Comune medesimo, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

9. Nei i casi indicati devono essere previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali degli interessati.

Art. 14 – Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. Il Titolare, in sede di pubblicazione e diffusione, tramite l'Albo pretorio informatico, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:

   a) sicurezza

   b) completezza

   c) esattezza

   d) accessibilità

   e) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità

   f) rispetto alle finalità perseguite.

2. Negli atti destinati alla pubblicazione o divulgazione, i dati che permettono di identificare gli interessati sono riportati solo quando è necessario ed è previsto da una norma di legge o, nei casi previsti dalla

legge, o da regolamenti o su consenso dell'interessato.

3. I sistemi informativi e i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estrazione degli atti, con l'esclusione dei dati personali in essi contenuti.

4. Se la valutazione preliminare porta a constatare che gli atti e i documenti resi conoscibili o pubblici devono contenere dati di carattere personale, al fine di rispettare il principio di pubblicità dell'attività amministrativa, deve essere rispettato il principio di proporzionalità, verificando se sono pertinenti e non eccedenti rispetto alle finalità perseguite.

5. Salva diversa disposizione di legge, il Titolare garantisce la riservatezza dei dati particolari in sede di pubblicazione all'Albo on line, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.

6. In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere particolare e/o relative a condanne penali e a reati, devono essere anonimizzati con adeguate tecniche.

7. I dati particolari e quelli relativi a condanne penali e a reati sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.

Art. 15- Pubblicazione web per obblighi di trasparenza

1. Il Titolare effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dal D.lgs. n. 33/2013 e ss.mm.ii.

2. I documenti di cui al comma 1 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e costantemente aggiornati.

3. Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni.

4. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.

5. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza.

6. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.

7. I dati vanno pubblicati in formato di tipo aperto, ai sensi dell'art. 68, D.Lgs. n. 82/2005 e sono liberamente riutilizzabili, secondo la normativa vigente. I dati personali diversi dai dati particolari e dai dati relativi a condanne penali e reati, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web.

8. I dati, le informazioni e i documenti di cui al comma 1, sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.

9. Deroghe alla predetta durata temporale quinquennale sono previste:

   a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;

   b) per alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale ai sensi dell'art. 14, comma 2, D.Lgs. n. 33/2013 e i titolari di incarichi dirigenziali e di collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D.Lgs. n. 33/2013;

   c) nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.

10. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

Art. 16 – Pertinenza delle informazioni contenenti dati personali

1. Il Titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

2. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico e dal relativo Regolamento Comunale sull'Accesso.

3. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

4. Non possono essere disposti filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente".

5. Qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto

all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza di terzi, l'accesso agli atti può essere limitato, su valutazione del Dirigente/ Responsabile del procedimento, mediante l'adozione di misure di sicurezza adeguate, compresa la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali e l'occultamento.

6. Il Dirigente /Responsabile del Procedimento destinatari dell'istanza di accesso possono consultare il DPO/RPD, al fine di garantire la massima protezione dei dati personali.

Art. 17 - Registro del trattamento

1. In attuazione del GDPR è istituito il Registro delle attività di trattamento **(Allegato 3)**, che identifica l'elenco delle attività di trattamento effettuate da questo Ente, i tipi di dati particolari e dati relativi a condanne penali e reati per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite (art. 30 GDPR);

2. Il DPO/RPD in caso di indicazioni cogenti del Garante della Privacy, dell'AGID o di altri organismi competenti, coordina l'attività degli uffici, al fine di aggiornare e modificare, secondo dette indicazioni, il registro di cui al comma precedente.

3. La compilazione e l'aggiornamento del Registro, a cadenza annuale, è curato dai Dirigenti, con il supporto del DPO/RPD e dello Staff Privacy.

4. Il Registro, su supporto cartaceo o in formato digitale, detenuto dal DPO/RPD, deve essere approvato con Deliberazione di Giunta Comunale.

5. Il Registro delle attività di trattamento, in quanto norma di organizzazione dell'Ente, costituisce anche una forma di autorizzazione al trattamento dei dati personali da parte dei soggetti riportati, sulla base di quanto previsto dall'art. 2-quaterdecies del D.Lgs. 30 giugno 2003, n. 196.

6. Il Registro contiene le seguenti informazioni:

a) dati di contatto del Titolare, del DPO/RPD e, dove del caso , del Contitolare del trattamento;

b) finalità del trattamento, le finalità per le quali sono trattati tali dati;

c) categorie di interessati;

d) categorie di dati personali;

e) categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

f) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, ove applicabile;

g) i termini ultimi previsti per la cancellazione delle diverse categorie di dati, ove possibile;

h) una descrizione generale delle misure di sicurezza tecniche e organizzative, ove possibile.

7. Anche i Responsabili del trattamento, che svolgono tali attività per conto del Titolare, sono obbligati a tenere e ad aggiornare analogo Registro.

8. Su richiesta, il Titolare o il Responsabile del trattamento, mettono il registro a disposizione del Garante.

Art. 18 - Fascicolo personale dipendenti e amministratori

1. I dati sullo stato di salute dei dipendenti e degli amministratori devono essere conservati separatamente rispetto alle altre informazioni personali. Il fascicolo, che raccoglie tutti gli atti relativi alla loro nomina, al percorso professionale e ai fatti più significativi che li riguardano, può mantenere la loro unitarietà, adottando accorgimenti che impediscano un accesso indiscriminato, quali l'utilizzo di sezioni o fascicoli dedicati alla custodia di eventuali dati particolari, da conservare chiusi o comunque con modalità che riducano la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

Art. 19 - Sensibilizzazione e formazione del personale

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

2. La formazione deve essere assicurata con la definizione, attuazione e controllo di un piano di formazione delle persone fisiche autorizzate al trattamento dei dati personali e che esso sia adeguato alla tipologia di trattamento; gli interventi di formazione e di aggiornamento in materia della riservatezza e protezione dei dati personali sono finalizzati alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento automatizzato e cartaceo, alla conoscenza di misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi e sulla *cyber security.*

3. A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è rappresentato dall'attività formativa ed informativa del personale dipendente, da curarsi da parte della Segreteria Generale con il supporto del DPO/RPD e dell'Ufficio Sistema Informativo-Informatico, nonché del Responsabile della prevenzione della Corruzione e della Trasparenza in merito al rapporto tra protezione dei dati e accesso civico alla documentazione amministrativa

4. Tutti i soggetti di cui al capo III sono destinatari degli interventi di formazione e di aggiornamento.

5. La partecipazione del personale dipendente agli interventi formativi è considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

CAPO IV ACCESSO AI DATI PERSONALI

Art. 20 - Trattamento interno dei dati personali

1. L'accesso ai dati personali da parte delle strutture e dei dipendenti, comunque limitato ai casi in cui è finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale il Titolare provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.

2. I soggetti rispondono delle azioni che ricadono sotto la propria responsabilità.

3. Compiti e responsabilità devono essere chiaramente definiti ed assegnati in modo inequivoco, formale e analitico. Ogni dipendente deve essere designato per specifici funzioni e compiti dal Titolare o da dirigente delegato alla designazione.

4. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale e dell'attività amministrativa.

5. I dirigenti, soprattutto se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone.

Art. 21- Utilizzo dei dati da parte dei Componenti gli Organi di Governo e di Controllo Interno

1. Il Sindaco, i Consiglieri comunali e gli Assessori nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti da questo Comune contenenti dati personali , nei limiti e con le modalità previsti dalle disposizioni di legge e di regolamenti.

2. Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della segretezza del loro contenuto.

Art. 22 - Trasmissione interconnessione e scambio di dati con altri soggetti

1. Il Titolare deve garantire che il trattamento dei dati personali si svolga nel rispetto del diritto alla riservatezza dell'identità personale degli interessati, favoriscono la trasmissione e lo scambio di dati o documenti tra le banche dati e gli archivi come previsto dalle normative nazionali ed europee in attività connesse alla realizzazione delle finalità di cui al precedente art. 4.

2. La comunicazione e l'interconnessione di banche dati, diverse da quelle ricomprese nelle particolari categorie di cui all'articolo 9 del GDPR e di quelle relative a condanne penali e reati di cui all'articolo 10 del GDPR, con altri soggetti pubblici per l'esecuzione di un compito di interesse pubblico o

connesso all'esercizio di pubblici poteri è ammessa, se prevista, ai sensi del comma 1 del d.lgs 196/2006. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali;

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 del d.lgs 196/2003

4. Qualsiasi richiesta è preceduta da protocollo d'intesa che contiene, di norma, l'indicazione del titolare, dei punti di contatto e delle operazioni di trattamento nonché le modalità di connessione, di trasferimento e di comunicazione dei dati e delle misure di sicurezza necessarie.

Art. 23 – Accesso ai dati personali da parte di soggetti privati.

1. Le richieste di soggetti privati intese ad ottenere il trattamento, la comunicazione e la diffusione dei dati personali nel rispetto delle norme, sono presentate in forma scritto e contengono:

   a) le generalità del richiedente;

   b) lo scopo e la finalità della richiesta;

   c) l'indicazione della banca dati;

   d) l'indicazione delle norme in base alle quali sussiste il diritto del richiedente.

2. Il Titolare valuta che la diffusione e la comunicazione sia legittima in base ad una norma di legge o, nei casi previsti dalla legge, da regolamento e che l'accoglimento dell'istanza non leda i diritti e le libertà fondamentali tutelati dal GDPR e dal Codice, con particolare attenzione a garantire il diritto alla riservatezza e all'identità personale dei soggetti cui i dati si riferiscono. In caso positivo, provvede alla trasmissione dei dati richiesti; in caso contrario emette provvedimento motivato di diniego.

3. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

4. Fatto salvo quanto previsto dal comma 3, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.

CAPO V DIRITTI DELL' INTERESSATO

Art. 24 – Diritti dell'interessato

1. Il Titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, in conformità alla disciplina contenuta nel GDPR e nel Codice.

2. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso, secondo la quale, l'interessato ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

   a) le finalità del trattamento;

   b) le categorie di dati personali in questione;

   c) i destinatari a cui i dati personali sono comunicati e qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate;

   d) il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

   e) l'esistenza del proprio diritto a richiedere la rettifica o cancellazione del dato o la limitazione dei dati o di opporsi al loro trattamento;

   f) il diritto di proporre reclamo a un'autorità di controllo;

   g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

   h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.

4. Il Titolare deve fornire risposta entro 30 giorni dal ricevimento della richiesta, termine che può essere prorogato di due mesi in casi di particolari complessità o ricorra un giustificato motivo, avvisando l'interessato del differimento, entro un mese dall'istanza.

5. L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

6. I diritti degli interessati possono essere ritardati, limitati o esclusi solo quando lo prevede una disposizione di legge e nel dettaglio:

   a) per non compromettere il buon esito dell'attività' di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, nonché l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza;

   b) per tutelare la sicurezza pubblica;

   c) per tutelare la sicurezza nazionale;

   d) per tutelare i diritti e la libertà altrui;

   e) quando è impossibile o è necessario uno sforzo spropositato;

   f) per una previsione normativa espressa;

   g) per tutela del segreto.

7. I soggetti di cui al capo III sono tenuti a collaborare per la verifica della sussistenza del diritto anche chiedendo informazioni all'interessato, per consentire l'esercizio del diritto.

Art. 25 – Modalità di esercizio dei diritti dell'interessato

1. In qualunque momento i cittadini possono far valere i diritti previsti dal regolamento generale sulla protezione dei dati 679/2016 dagli artt. 15 e successivi

2. Il Titolare mette a disposizione dell'utente un modulo standard per la richiesta di accesso. L'uso di un formato o di un modulo diverso da quello presente sul sito comunale non comporta l'inammissibilità o il rigetto, purché siano rispettate tutte le formalità ivi contenute

3. Il modulo di richiesta per l'esercizio dei diritti (**Allegato 4)**, pubblicato sul sito istituzionale-Amministrazione Trasparente, altri contenuti può essere fatto pervenire:

   - direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;

- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;

- tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;

- in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;

- dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.

4. L'interessato può presentare o inviare la richiesta di esercizio dei diritti, intestata al Sindaco:

   - all'Ufficio Protocollo Generale del Comune di Potenza - Via N. Sauro; Posta Elettronica Certificata: protocollo@pec.comune.potenza.it che provvederà all'assegnazione al Dirigente competente.

   - all'Ufficio per le Relazioni con il Pubblico: Piazza Matteotti -85100 Potenza; urp@comune.potenza.it

5. La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.

6. La richiesta sarà soddisfatta, salvo diversa indicazione dell'interessato, utilizzando gli stessi canali di trasmissione (supporto cartaceo o canali telematici)

7. I soggetti competenti alla valutazione dell'istanza sono il Dirigente competente il quale decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati, avvalendosi anche, laddove ritenuto necessario, della consulenza del DPO/RPD.

Art. 26 – Indagini difensive

1. Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di procedura penale, può chiedere documenti in possesso del Titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.

2. Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina al Regolamento comunale sul diritto di accesso.

3. Il Titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

Art. 27 - Obbligo di informativa

1. Prima che inizi qualunque trattamento di dati personali, il Titolare fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.

2. L'informativa sul trattamento dei dati personali deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.

3. L'informativa **(Allegato 5)** deve essere fornita:

    a) in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;

    b) in caso di dati personali non ottenuti presso l'interessato;

    c) entro un termine ragionevole, massimo di un mese dalla raccolta (non registrazione) dei dati;

    d) nel caso in cui i dati vadano comunicati all'interessato alla prima comunicazione;

    e) se i dati personali devono essere comunicati ad un altro destinatario, non oltre la prima comunicazione.

4. Non è necessario fornire l'informativa:

    a) nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;

    b) nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni.

5. Il Titolare ha la facoltà di aggiungere ulteriori informazioni ritenute necessarie, nei casi di specie.

Art. 28 – Modulistica e procedure

1. Il Titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del GDPR, del presente Regolamento e di tutte le linee guida e provvedimenti del Garante:

    a) adotta e costantemente aggiorna:
    - modelli uniformi di informativa;
    - modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;

    b) elabora, approva, e costantemente aggiorna adeguate procedure gestionali.

CAPO VI MISURE DI SICUREZZA

Art. 29 – Piano di Protezione dei dati personali e gestione del rischio di violazione

1. In base al principio di responsabilizzazione (*accountability)*, introdotto dal GDPR e dal d.. lgs. 10 agosto 2018, n. 101 il Titolare e il Responsabile del Trattamento, individuano adeguate misure, tecniche e organizzative, a tutela dei dati trattati

2. Il Titolare, pertanto, provvede a dotarsi, su base volontaria, di un Piano di protezione dei dati (PPD), idoneo a prevenire trattamenti illeciti e violazioni attribuibili a vulnerabilità della sicurezza.

3. Il piano di protezione dei dati personali e gestione del rischio di violazione da redigere con cadenza biennale , da parte dello Staff Privacy, con il coordinamento del DPO/RPD , descrive le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche/logiche, logistiche/fisiche, organizzative e procedurali da adottare e da applicare per ridurre/eliminare il rischio di violazione dei dati derivante dal trattamento.

Art. 30 - Misure di sicurezza

1. Il Titolare mette in atto misure tecniche ed organizzative adeguate a 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.

2. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento, derivanti, in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. All'uopo sarà predisposta una idonea procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative, al fine di garantire la sicurezza del trattamento, rivolgendosi anche a soggetti terzi.

3. Il comma 2, in particolare e tutto il capo delle misure di sicurezza in generale, tiene conto del Considerando 78, ovvero quanto elaborato in dottrina in termini di sistema privacy by design e by default. Per privacy by design si intende un sistema che prima del trattamento dei dati adotta misure per incrementare la sicurezza, quali le tecniche di anonimizzazione e pseudonimizzazione. Per privacy by default si intende un'applicazione del principio di minimizzazione dell'uso dei dati personali; ovvero, trattamento dei soli dati necessari per ogni specifica finalità (massima protezione dei dati attraverso il loro minimo trattamento).

4. Nella gestione dei dati personali con il sistema informatizzato dovrà essere assicurato il puntuale e scrupoloso rispetto di tutte le norme vigenti e la definizione di procedure e linee guida da parte

dell'Ufficio Sistema Informatico-Informativo comunale.

5. Per il trattamento di dati personali effettuato con strumenti elettronici sono da considerate tutte le misure idonee al trattamento, come da Allegato 2, e riservandosi, se necessario, con opportuna valutazione di impatto (DPIA), l'introduzione di nuove misure di sicurezza, più idonee alla gestione del rischio del trattamento dati personali in considerazione.

6. Ogni ulteriore misura idonea a tutela delle banche dati personali informatiche o cartacee andrà adottata secondo un principio di proporzionalità tra le risorse disponibili e i diritti da tutelare.

7. Per la mitigazione del rischio, proveniente da vulnerabilità, è necessario, attuare misure tecniche e organizzative, sentito l'Amministratore di sistema.

8. I Dirigenti si attivano periodicamente con controlli, anche a campione, al fine di garantire la sicurezza delle banche dati e l'esattezza e completezza dei dati inseriti.

9. Per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto, il Titolare favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, nonché a meccanismi di certificazione della protezione dei dati, anche stipulando contratti con società terze, dotate di adeguate competenze professionali, al fine della valutazione periodica della sicurezza del sistema informatico.

10. Il Titolare si obbliga a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca ed abbia accesso a dati personali.

Art. 31 – Valutazione di impatto sulla protezione dei dati personali (DPIA)

1. È redatta una valutazione di impatto sui dati personali (DPIA- art. 35 GDPR) quando la tipologia di trattamento, definita nel registro delle attività di trattamento, "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1).
2. L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati, a cadenza annuale, è in capo ai Dirigenti, con il coordinamento dello Staff Privacy, del Servizio Informativo-Informatico.
3. Al fine di valutare i trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone, per questo soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, si seguiranno le *"linee guida" in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (di seguito "WP 248, rev. 01"* e l'*allegato 1 al provvedimento n. 467 del'11 ottobre 2018 [doc. web. N. 9058979] e comunque ogni altra disposizione o linee giuda redatti o pubblicati dal Garante Privacy;*
4. La DPIA conterrà quanto definito all'articolo 35, paragrafo 7, come segue:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione

5. Il Titolare deve consultarsi con il DPO/RPD, e il parere ricevuto, così come le decisioni prese dal Titolare, devono essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il DPO/RPD deve altresì sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati (articolo 39, paragrafo 1, lettera c)).

6. Il DPO/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.

7. Qualora il trattamento venga eseguito in toto o in parte da un Responsabile del trattamento dei dati, quest'ultimo deve assistere il Titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie

8. 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 (Azioni non autorizzate, Compromissione informazioni, Problemi tecnici ed interruzione di servizi, Eventi naturali) del trattamento dei dati personali;

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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

9. 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.

10. 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 taluni trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

11. 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.

Art. 32 - Pubblicazione sintesi della valutazione d'impatto (D.P.I.A.)

1. Il Titolare effettua la pubblicazione della D.P.I.A. o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati, nonché di dimostrare la responsabilizzazione e la trasparenza.

2. La D.P.I.A. pubblicata non deve contenere l'intera valutazione, qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza o a divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere

soltanto in una sintesi delle principali risultanze o in una dichiarazione che attesti la realizzazione della stessa.

Art. 33 - Sistema e politica di audit

1. Il Titolare mette in atto misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è conforme al GDPR e, a tal fine, adotta il procedimento di audit in conformità anche delle politiche della qualità.
2. Il Titolare definire un programma di audit di durata triennale.
3. Ogni piano di audit dovrà definire:

   a) le modalità tecniche di campionamento degli atti, delle procedure amministrative e dei contratti, anche in modo differenziato per tipologia e valore;

   b) gli indicatori e i parametri di verifica per ciascuna tipologia di atti;

   c) la percentuale di atti da verificare;

   d) le modalità per assicurare il coinvolgimento dei dirigenti.

4. Il Titolare, con il supporto del DPO/RPD e dello Staff Privacy, valuta, mediante gli audit, i processi interni per:

   a) verificare il grado di conformità del trattamento dei dati personali effettuato da tutti gli uffici alla normativa vigente;

   b) verificare che tutti i dipendenti osservino le regole per la liceità e la sicurezza del trattamento di dati personali;

   c) verificare l'efficacia di azioni correttive a seguito di "non conformità".

5. Il piano di audit dovrà considerare, testare, valutare e confrontare i seguenti elementi:
   a) politiche, procedure e piani di sicurezza dell'organizzazione;
   b) risultati di precedenti verifiche interne o esterne;
   c) risultati della valutazione del rischio, attuazione dei controlli, valutazione dell'impatto sulla protezione dei dati, ecc.;
   d) controlli applicabili dalla norma ISO 27001, 27002, 31000, 29134;
6. Il processo del comma precedente, dopo la prima volta che è stato effettuato, si sviluppa in monitoraggi periodici di verifica dell'applicazione delle misure stabilite e nella sostituzione o riesame delle misure per il miglioramento dei trattamenti da parte dei vari uffici del Comune.

Art. 34 - Procedimento di audit

1. Il DPO/RPD e il Referente interno della Privacy, procedono nell'audit mediante:
   a) somministrazione di questionari ed interviste ai soggetti di cui al capo II
   b) consultazione delle banche dati ed archivi informatici e cartacei del Comune;

2. A seguito dell'attività di cui al comma precedente, vengono analizzati i risultati emersi che possono consistere in:
   a) situazioni di conformità;
   b) raccomandazioni per il miglioramento;
   c) situazioni di non conformità.
3. Tali risultati vengono formalizzati in un rapporto di audit che dà atto di tutte le fasi del procedimento svolto e fornisce al Titolare e/o al Responsabile del trattamento l'indicazione delle eventuali azioni correttive da porre in essere

CAPO VII *DATA BREACH* O VIOLAZIONE DEI DATI PERSONALI

Art. 35 –Definizione di violazioni dei dati personali

1. Una violazione di dati personali *(Data Breach)* è 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

2. Le violazioni possono essere classificate in base ai seguenti tre principi:

   a) violazione della riservatezza, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

   b) violazione dell'integrità, in caso di modifica non autorizzata o accidentale dei dati personali;

   c) violazione della disponibilità, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

3. Ogni violazione di dati personali deve essere documentata in un apposito registro **(Allegato 6)**

Art. 36 – Notifica violazioni dei dati personali

1. Il Titolare deve notificare la violazione all'autorità di controllo competente **(Allegato 7).**, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche e impone altresì che, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa venga corredata dei motivi del ritardo;

2. Il Titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio posto che tale documentazione consente all'autorità di controllo di verificare il rispetto della disciplina in tema di notifiche di violazioni;

3. Il Responsabile del trattamento deve informare il titolare del trattamento, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione. L'articolo 33, paragrafo 2 del GDPR chiarisce che

se il Titolare ricorre a un Responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare, deve notificarla a questi "senza ingiustificato ritardo".

4. Il Responsabile del trattamento non deve valutare la probabilità di rischio derivante dalla violazione prima di notificarla al Titolare, spettando infatti a quest'ultimo effettuare la valutazione nel momento in cui viene a conoscenza della violazione. Il Responsabile del trattamento che ha accertato una violazione di dati personali segnala la stessa al Titolare del trattamento, compilando apposito modulo (**Allegato 8).**

Art. 37 – Comunicazione di una violazione dei dati personali agli interessati

1. Il Titolare del trattamento deve comunicare senza ingiustificato ritardo quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, salve le eccezioni previste dall'art. 34 par. 3 GDPR.

2. La comunicazione deve contenere, ai sensi dell'art. 34, le seguenti informazioni:

   a) il nome e i dati di contatto del DPO/RPD o di altro punto di contatto;

   b) la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

CAPO VIII MEZZI DI TUTELA E RESPONSABILITA'

Art. 38 - Soggetti responsabili ed azione risarcitoria

1. Il Titolare è responsabile per ogni danno materiale o immateriale causato da una violazione dei dati personali trattati ed è tenuto a risarcire l'interessato o la persona fisica e giuridica danneggiata.

2. All'obbligazione risarcitoria è tenuto verso il danneggiato anche il Responsabile del trattamento se il danno è stato causato da un suo inadempimento nell'ambito dei compiti a cui è stato preposto.

3. Il Titolare e il Responsabile del trattamento sono esenti da responsabilità se provano che l'evento dannoso non è loro imputabile.

4. L'azione risarcitoria va proposta dinanzi all'autorità giudiziaria ordinaria secondo le norme dell'ordinamento interno.

5. Il DPO/RPD non risponde nei confronti dei danneggiati ma solo nei confronti del Titolare e in relazione alle specifiche competenze attribuite al momento del conferimento dell'incarico e con successivi accordi scritti.

Art. 39- Reclamo

1. Fatta salva la tutela giurisdizionale, l'interessato può presentare reclamo al Garante se ritiene che il Titolare abbia violato la riservatezza dei propri dati.

2. Il reclamo è presentato in forma scritta senza particolari formalità al Garante e contiene la documentazione utile per la valutazione nonché le informazioni sul Titolare e sul Responsabile di trattamento oltre che dell'interessato.

3. Il Garante effettua un'istruttoria preliminare in cui può richiedere informazioni al Titolare e all'esito del procedimento può imporre allo stesso di adottare i provvedimenti necessari per rendere il trattamento dei dati conforme alla disciplina vigente.

4. Il Garante informa l'interessato dello stato o dell'esito di reclamo.

Art. 40 - Trattamento illecito dei dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla protezione dei dati personali, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla materia è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni e la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 167 e 172, D.Lgs. n. 196/2003.

Art. 41- Falsità nelle dichiarazioni e notificazioni al Garante della privacy

1. I Dirigenti o il DPO/RPD, in esecuzione delle rispettive competenze, procedono per conto del Titolare con notificazioni, comunicazioni al Garante, qualora forniscano false dichiarazioni o attestazioni o producono documenti falsi, salvo che il fatto costituisca reato più grave, sono puniti con la reclusione da sei mesi a tre anni e la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 168 e 172, D.Lgs. n. 196/2003.

Art. 42 - Omessa predisposizione di misure di sicurezza

1. Il Titolare e le persone fisiche che agiscono per suo conto che non adottano le misure di sicurezza minime sono penalmente responsabili e sono puniti con arresto fino a due anni dalle autorità giudiziarie competenti, oltre con la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 169 e 172, D.lgs. n. 196/2003.

CAPO IX ENTRATA IN VIGORE E DISPOSIZIONI FINALI

Art. 43 - Entrata in vigore del regolamento

1. Il presente regolamento entra in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione.

2. Il regolamento e la relativa modulistica per l'esercizio dei diritti sono resi pubblici mediante pubblicazione sul sito internet del Comune, nella Sezione Amministrazione Trasparente " Regolamenti"

Art. 44 – Disposizioni finali

1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.

2. Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.