Regolamento per la protezione dei dati personali e particolari

Adottato, con delibera dell'Amministratore Unico p.t. n. 10/2019 del 04/03/2019, a norma del D.Lgs. 30 giugno 2003 n. 196: "*Codice in materia di protezione dei dati personali***" e aggiornato al Regolamento UE 2016/679 del 27 aprile 2016 relativo alla "***Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"***.**

Art. 1 - Oggetto del regolamento

1. Il presente Regolamento disciplina le misure tecniche e organizzative sul trattamento dei dati personali contenuti nelle banche dati organizzate, gestite o utilizzate dall'Azienda Territoriale per L'Edilizia Residenziale della Provincia di Potenza, in relazione allo svolgimento delle proprie finalità con riguardo ai trattamenti dei dati personali e particolari, nonché alla libera circolazione di tali dati, in attuazione:
   - del Regolamento UE 2016/679 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;
   - del D.Lgs. 30 giugno 2003, n.196, recante "Codice in materia di protezione dei dati personali";
   - del D.Lgs.10/08/2018 n.101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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);
   - della normativa in materia di diritto di accesso documentale, accesso civico e accesso generalizzato.

Art. 2 – Finalità

1. L'Azienda Territoriale per L'Edilizia Residenziale della Provincia di Potenza, 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 svolge 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, favorisce la trasmissione di dati e documenti tra le proprie banche dati ed archivi e quelli degli enti territoriali, degli enti pubblici, dei gestori e degli 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 della Azienda Territoriale per L'Edilizia Residenziale della Provincia di Potenza si intendono le funzioni ad essa attribuite dalle leggi, dallo statuto e dai regolamenti, anche svolte per mezzo di intese, accordi, convenzioni.
5. Il presente Regolamento definisce le politiche di questa Amministrazione su:
   - attuazione delle procedure articolate per "Informare le persone" degli scopi della raccolta;
   - necessità di valutare quale sia la base giuridica idonea a legittimare ogni trattamento di dati personali dell'organizzazione;
   - limitazione della raccolta di informazioni personali (sia in termini di quantità e tipo di informazioni) rispetto a quanto necessario per le finalità identificate, assicurando che vengano raccolte con mezzi legittimi;
   - conservazione e distruzione di informazioni personali (dove conservarle, chi può accedere, per quanto tempo);
   - modalità atte a garantire che le informazioni siano corrette, complete e aggiornate (metadatare tutte le informazioni e permettere agli individui di chiedere rettifiche in maniera facile);
   - predisposizione di misure di sicurezza adeguate;
   - strumenti per rendere disponibili informazioni al pubblico mediante politiche e pratiche condivise;
   - modalità di ricezione ed elaborazione delle richieste di accesso;
   - modalità di ricezione e risposta a richieste e reclami.

6. Il presente Regolamento definisce le politiche amministrative per la governance e la gestione della privacy che definiscano le aspettative in merito a:
   - strutture organizzative, ruoli e responsabilità e istruzioni per raggiungere i requisiti di privacy;
   - politiche e procedure di gestione dei rischi;
   - assegnazione di risorse sufficienti e appropriate per attuare e supportare le politiche sulla privacy;
   - valutazioni dell'impatto sulla privacy prima che vengano introdotti nuovi servizi o sistemi informativi o verificare quelli già in corso (valutazioni di impatto per i trattamenti più a rischio);
   - norme di sicurezza e gestione delle informazioni per garantire che le informazioni siano protette contro la divulgazione, la modifica, l'interruzione, la rimozione o la distruzione non autorizzate;
   - revisione periodica della progettazione, dell'acquisizione, dello sviluppo, dell'implementazione, della configurazione e della gestione dell'infrastruttura, dei sistemi, delle applicazioni e dei siti Web per garantire la coerenza con le politiche e le procedure sulla privacy;
   - risoluzione dei data breach e delle cause di violazioni della privacy, compresa la perdita di informazioni personali o l'uso inappropriato di informazioni personali;
   - risposte ai reclami sulla privacy ed adozione di misure correttive;
   - formazione sulla privacy del personale dipendente e a contratto;
   - conformità con buone pratiche di gestione della privacy (adesione a codici di condotta o certificazioni).

Art. 3 - Definizioni

1. Ai fini del presente regolamento si intende per:
   a. *"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;
   b. "*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;
   c. "*Identificazione/Identificabilità"* - Identificata/identificabile è una condizione della persona, rispettivamente effettiva (identificata) o possibile (identificabile);
   d. "*Dato pluripersonale"* - Dato che può essere collegato a più soggetti, dunque presentare una pluralità di interessati;
   e. "*Dati particolari*" - Trattasi 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;
   f. "*Dati relativi a condanne penali e reati"* - Trattasi 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;
   g. "*Titolare del trattamento*" - La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

h. "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;

i. "A*utorizzati"* - 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;

j. "R*esponsabile della banca dati"* - Le persone fisiche a cui sono attribuiti specifici compiti connessi al trattamento di dati personali, con funzioni apicali 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 e che devono garantire il rispetto delle disposizioni del presente regolamento;

k. "Interessato*"* - La persona fisica identificata o identificabile cui si riferiscono i dati personali;

l. "Comunicazione*"* - 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;

m. "Diffusione*"* - Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n. *"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 sono oggetto di trattamento;

o. **"**Informazione anonima*"* - Informazione che non riguarda una persona fisica identificata o identificabile;

p. **"**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;

q. **"**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;

r. "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;

s. "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*);

t. "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;

u. "Diritto di rettifica e integrazione*"* - Diritto di vedere i propri dati accurati e ed esatti;

v. "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;

w. "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;

x. "Autorità di controllo*"* - L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

y. "Autorità di controllo interessata": - Un'autorità di controllo interessata dal trattamento di dati personali in 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 reclamo è stato proposto a tale autorità di controllo;

z. "Comunicazione elettronica" - Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

aa. "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;

bb. "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;

cc. "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;

dd. "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);

ee. "Ponderazione del rischio"- Processo di comparazione dei risultati dell'analisi del rischio, rispetto ai criteri di rischio per determinare se lo stesso e/o la sua espressione quantitativa sia accettabile o tollerabile;

ff. "Processo"- Insieme di attività tra loro correlate o interagenti le quali trasformano gli input in output;

gg. "Profilazione"- Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati 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;

hh. "Pseudonimizzazione"- Trattamento dei dati personali in modo tale che gli stessi 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;

ii. "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;

jj. "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;

kk. "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;

ll. "Valutazioni"- Processo complessivo di identificazione, analisi e ponderazione del rischio;

mm. "Chiamata" Connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;

nn. "Reti di comunicazione elettronica"- Sistemi di trasmissione e, se del caso, 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;

oo. "Rete pubblica di comunicazioni"- 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;

pp. "Servizio di comunicazione elettronica" - 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;

qq. "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;

rr. "Utente" - Persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

ss. "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;

tt. "Dati relativi all'ubicazione" – Ogni altro 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;

uu. "Dati genetici" - 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;

vv. "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;

ww. "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;

xx. "Servizio a valore aggiunto" - 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;

yy. "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;

zz. "Misure di sicurezza" - Misure tecniche ed organizzative adeguate a garantire la sicurezza di ogni trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche;

aaa. "Strumenti elettronici" - Elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

bbb. "Autenticazione informatica" - Insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

ccc. "Credenziali di autenticazione" - Dati e dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

ddd. "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;

eee. "Profilo di autorizzazione" - Insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

fff. "Sistema di autorizzazione"- 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;

ggg. "Violazione di dati personali" - 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;

hhh. "Scopi storici" - Finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

iii. "Scopi statistici" - Finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

jjj. "Scopi scientifici" - Finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore;

kkk. "Obiezione pertinente e motivata" - Obiezione rispetto ad un provvedimento o ad un'attività dell'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. 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. E' necessario determinare le finalità dei trattamenti di dati personali coerentemente con gli obbiettivi istituzionali e di gestione del sistema informativo.
3. I trattamenti effettuati dall'Amministrazione 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, 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. L'Amministrazione 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 l'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 sia 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. Nel caso in cui un trattamento di dati personali sia necessario per l'esecuzione di compito di interesse pubblico o connesso all'esercizio di pubblici poteri ma manchi una norma di legge o di regolamento, il titolare del trattamento o un suo delegato, sentito il Data Protection Officer, può attivarsi solo dopo aver interpellato l'Autorità Garante nei modi dell'art. 2-ter del Codice della pivacy, come modificato dal D.Lgs. n.101/2018 solo nel caso in cui si trattino:
    a. Dati comuni;
    b. Tipologia di trattamento unicamente "comunicazione".
9. 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.

Art. 5 – Titolare del Trattamento

1. L'Azienda Territoriale per L'Edilizia Residenziale della Provincia di Potenza, rappresentata ai fini previsti dal GDPR dall'Amministratore Unico pro-tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). L'Amministratore Unico può delegare le relative funzioni al Dirigente in possesso di adeguate e comprovate competenze.
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 adotta 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 finanziaria generale dell'Ente (bilancio e PEG), previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
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 (di seguito indicata con l'acronimo "DPIA" *Data Protection Impact Analysis*) ai sensi dell'art.35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 21.
7. Il Titolare, inoltre, provvede a:
   a. designare espressamente, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, le persone fisiche autorizzate al trattamento dei dati personali, ciascuno in relazione ai procedimenti amministrativi singolarmente assegnati;
   b. nominare il Responsabile della Protezione dei Dati (di seguito RDP/DPO *Data Protection Officer*);
   c. nominare, quale Responsabile del trattamento, i soggetti pubblici o privati affidatari di attività e servizi per conto dell'organizzazione, relativamente alle banche dati gestite da soggetti esterni all'azienda in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;
   d. predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente;
   e. valutare casi di contitolarità prima dell'inizio del trattamento dei dati personali e stipulare accordi con i contitolari secondo l'art.26 del GDPR.
8. L'azienda favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per

contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 6 – Data Protection Officer (DPO)

1. L'Azienda si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD/DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità tecnica specialistica di assolvere i compiti di competenza.
2. L'Azienda non può procedere nella sua attività istituzionale senza un Data Protection Officer espressamente designato dall'Amministratore Unico o da un suo delegato.
3. Il Data Protection Officer può essere un dipendente in posizione apicale oppure un incaricato che potrà assolvere i suoi compiti in base a un contratto di servizio previo espletamento di procedura ad evidenza pubblica.
4. In caso di DPO 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 nomina a DPO presuppone l'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del DPO.
6. Sul sito istituzionale vanno pubblicati i dati di contatto del DPO e vanno comunicati al Garante della protezione dei dati personali.
7. Il DPO 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 per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
9. Il DPO 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 all'Amministratore Unico, al Direttore, 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 dei titolari del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
    c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
    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 è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione con onere di comunicazione di detto adempimento al Titolare del trattamento.
11. Per le refluenze sulla governance dell'Azienda, il DPO per le competenze ascrittegli che richiedono adeguata conoscenza giuridica e informatica, professionalità nonché approfondita conoscenza delle strutture organizzative dell'Ente e dall'Ufficio Trattamento Dati di cui al successivo art. 10.
12. Il Titolare ed il Responsabile del trattamento assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
    - il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
    - il DPO deve ricevere tempestivamente tramite posta elettronica, dal Titolare e dal Responsabile del trattamento dati tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea;

- il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione;
- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente (Data Breach); egli con proprio parere indica quali provvedimenti debbano essere adottati per porre rimedio ovvero per prevenire il ripetersi di tali violazioni.

13. Nello svolgimento dei compiti affidatigli il DPO 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:
    a. procede ad una mappatura delle aree di attività, valutandone il grado di rischio in termini di protezione dei dati ed 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.
14. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Azienda.
15. La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
    - il Responsabile per la prevenzione della corruzione e il Responsabile per la trasparenza;
    - il Responsabile del trattamento dati;
    - qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.
16. Il Titolare ed il Responsabile del trattamento forniscono al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al DPO:
    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, specializzato in materia tramite la costituzione di una apposita unità organizzativa denominata "Ufficio Trattamento Dati Personali" di cui al successivo art.10;
    c. 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;
    d. l'accesso garantito ai settori funzionali dell'Azienda, così da fornirgli supporto, informazioni e input essenziali.
17. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare.
18. Il DPO è tenuto a manifestare il proprio dissenso alle decisioni o ai provvedimenti o ai 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 all'Amministratore Unico, al Direttore, ai Responsabili del trattamento interessati dai rilievi e, ove necessario, al Gestore informatico. I Responsabili del trattamento, qualora non condividano i rilievi formulati dal DPO, comunicano a quest'ultimo e all'Amministratore Unico le proprie osservazioni. Il DPO dirama le direttive utili a prevenire il ripetersi delle violazioni rilevate.
19. Il DPO non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.
20. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 7 – Contitolarità del trattamento

1. Il Regolamento UE 679/2016 disciplina con l'art. 26 l'ipotesi in cui Il trattamento dei dati personali può essere effettuato da uno o più titolari.
2. Nel caso in cui l'organizzazione identifichi una situazione di "contitolarità" del trattamento e cioè quando "due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento" è necessario prevedere un accordo scritto con il quale si disciplinano le responsabilità, il rispetto degli obblighi previsti dal Regolamento UE 679/2016 e i ruoli.
3. Gli accordi di contitolarità dovranno indicare in maniera trasparente le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento UE 679/2016, 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 designare un punto di contatto per gli interessati.

Art. 8 – Responsabili del Trattamento

1. L'Azienda 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 l'Azienda 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 maniera scritta gli obblighi delle parti preposte alle attività di trattamento, definendone modalità, condizioni, durata, natura e finalità e chiarendo espressamente il tipo di dati personali trattati, le categorie di interessati, nonché gli obblighi e i diritti del titolare del trattamento 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, che possono avere solo la forma scritta e con atto vincolante per il responsabile del trattamento, dovrebbero 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 Regolamento, 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. 9 – Limitazione degli adempimenti non necessari e "Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati e valutazione di impatto sulla protezione dei dati"

1. Il DPO deve:
   a. Vigilare e richiamare tutti i dipendenti e i relativi responsabili degli uffici al corretto adempimento di tutte le disposizioni di legge a tutela della riservatezza dei dati personali;
   b. Controllare che nessun dipendente e nessun responsabile degli uffici adotti comportamenti o richieda adempimenti in materia di tutela della riservatezza dei dati personali, non obbligatori in base alla normativa vigente, alle disposizioni del Garante della privacy e al presente regolamento.
2. Nell'ottica di non appesantire l'attività degli uffici con adempimenti non obbligatori e di coordinare attività con finalità simili al fine della massimizzazione delle risorse umane e strumentali, deve essere redatto e aggiornato il "*Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati e valutazione di impatto sulla protezione dei dati*" (Allegato 1).
3. Il DPO, in caso di indicazioni cogenti del Garante della Privacy, dell'AGID o di altri organismi dalle competenze simili, dovrà coordinare l'attività degli uffici al fine di aggiornare e modificare, secondo dette

indicazioni, il registro di cui al comma precedente.

4. La compilazione e l'aggiornamento deve essere effettuato almeno una volta per anno solare, delle varie parti del registro, dai Responsabili delle Banche dati, coordinata dal DPO e dall'Ufficio Trattamento dei Dati.
5. L'aggiornamento dovrà essere approvato mediante un'apposita deliberazione dell'Amministratore Unico.
6. Il DPO assegna un termine a ciascun dirigente per aggiornare e compilare apposite schede di autovalutazione afferenti alle banche dati affidate alla gestione di detti soggetti; una volta compilate e aggiornate si provvederà alla stesura del nuova versione del registro delle attività di trattamento e la sua pubblicazione sul sito istituzionale nella stessa sezione di "Amministrazione trasparente".
7. Il registro dovrà avere forma cartacea e digitale secondo le esigenze e le dotazioni disponibili al momento dell'adozione.
8. La mancata formulazione o aggiornamento delle schede di autovalutazione afferenti ai trattamenti comporta responsabilità del dirigente apicale preposto al settore di competenza.
9. Le schede di autovalutazione sono inoltrate ad ogni dipendente dal dirigente apicale, una per ogni trattamento da lui svolto. Ogni scheda contiene elementi per l'autovalutazione. La mancata compilazione delle schede di autovalutazione dei trattamenti comporta violazione dei doveri di ufficio e verrà considerata ai fini della valutazione della performance nonché fonte di responsabilità civile, a carico dell'inadempiente, a norma dell'art. 82 del Regolamento UE.
10. I soggetti autorizzati al trattamento dal titolare del trattamento dovranno identificare e documentare nel dettaglio le finalità del trattamento prima o al momento della raccolta.
11. I soggetti interessati dovranno essere adeguatamente informati sulle finalità del trattamento.
12. Le persone autorizzate al trattamento devono determinare le quantità e i tipi di informazioni che devono essere raccolte per poter adempiere agli scopi.
13. Le persone autorizzate al trattamento devono poter dimostrare che i motivi per cui si stanno raccogliendo informazioni personali sono quelli che una persona ragionevole si aspetterebbe o riterrà opportuno in normali circostanze;

Art. 10 – Ufficio Protezione Dati Personali

1. L'Ufficio Protezione Dati Personali, da incardinarsi nell'Area della Direzione dell'Azienda e le cui competenze verranno meglio descritte nel Regolamento di Organizzazione, costituisce l'unità organizzativa preposta a garantire l'uniformità di applicazione del GDPR e del presente Regolamento, fornendo il necessario supporto tecnico-amministrativo al Titolare del trattamento e al DPO. Il Titolare del trattamento deve assicurare all'Ufficio Protezione Dati Personali le risorse umane, finanziarie e tecnico-informatiche necessarie per assolvere ai compiti assegnati.
2. Specifici compiti dovranno essere svolti dall'Ufficio Protezione Dati Personali, presieduto dal DPO stesso e dal Referente interno della privacy dell'Azienda, nominato dall'Amministratore Unico, competente in materia di governance e gestione della protezione dei dati personali e che occupi un livello gerarchico sufficientemente elevato e da personale qualifica in materia privacy e tutela dei dati personali. Lo staff dovrà adempiere almeno ai seguenti compiti:
    a. tenere aggiornato il presente Regolamento sulla protezione dei dati personali, in conformità con la normativa europea e nazionale;
    b. curare la comunicazione interna ed esterna relativa alle tematiche della privacy;
    c. monitorare il rispetto delle politiche in materia di protezione dei dati personali, attraverso questionari di autovalutazione, attività di audit interno, o con riguardo alla gestione di reclami, richieste o possibili violazioni;
    d. svolgere attività di front-end per ogni reclamo diretto all'Azienda;
    e. mantenere aggiornato il "Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati comunali e valutazione di impatto sulla protezione dei dati" in linea con quanto prescritto dall'art.30 del Regolamento UE 679/2016;

f. svolgere ogni altro compito previsto dal Regolamento di Organizzazione.

Art. 11 – Interazioni con amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale

1. Il Responsabile della protezione dei dati personali e il Responsabile per la prevenzione della corruzione e della trasparenza tutte le volte che procedimenti interni o attivati da soggetti esterni abbiano delle interazioni tra le attività di pubblicazione dei dati personali in amministrazione trasparente, il rilascio di dati personali in occasione di istanze di accesso civico, generalizzato e documentale, dovranno coordinare la loro azione al fine di minimizzare l'impatto degli adempimenti sull'attività degli uffici e garantire la massima protezione dei dati personali.

Art. 12 - Formazione del personale

1. Il Responsabile della protezione dei dati personali, il Responsabile per la prevenzione della corruzione e della trasparenza e il Responsabile per la Transizione digitale, qualora l'Amministratore Unico dovesse provvedere a nominare due soggetti diversi, insieme con l'ufficio del SIA e l'Ufficio Protezione Dati Personali, dovranno coordinare e attuare misure di formazione del personale, anche con riscontro dell'acquisizione di abilità e competenze, al fine di garantire, nell'attività degli uffici, il massimo di trasparenza possibile e l'assoluto rispetto dei diritti di riservatezza dei dati personali dei cittadini e dipendenti.
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.

Art. 13 - Trattamento interno dei dati personali

1. Le disposizioni del presente Regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno. L'accesso ai dati personali da parte delle strutture e dei dipendenti, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale l'ATER 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, nei vari livelli dell'organizzazione, rispondono delle azioni che ricadono sotto la loro responsabilità.
3. Compiti e responsabilità devono essere chiaramente definiti ed assegnati in modo chiaro, inequivoco, formale ed analitico. Ogni dipendente deve essere designato per specifici funzioni e compiti dal titolare del trattamento o da un suo delegato con provvedimento pubblicato, per la massima trasparenza e accessibilità sul sito istituzionale dell'organizzazione nella sezione amministrazione trasparente nella apposita sotto sezione *(Organizzazione/ Articolazione degli uffici)*.
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.
5. Il responsabile della banca dati, specie se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone.

Art. 14 Utilizzo di Dati da parte dei Componenti gli Organi di Governo e di Controllo Interno

1. L'Amministratore Unico, il Direttore, nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti da questa Azienda contenenti dati personali detenuti dalla società 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. 15 - Trasmissione interconnessione e scambio di dati con altri soggetti

1. L'organizzazione e le sue articolazione a carattere autonomo devono garantire che il trattamento dei dati personali si svolga nel rispetto del diritto alla riservatezza dell'identità personale degli interessati, favoriscano 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. Le operazioni di interconnessione e raffronto con banche dati di altri titolari del trattamento e di comunicazione a terzi sono ammesse solamente se indispensabili allo svolgimento di obblighi o compiti della società e solo per il perseguimento di finalità di interesse pubblico.
3. Le operazioni di cui al primo comma sono svolte nel rispetto delle disposizioni in materia di protezione dei dati personali e degli altri limiti stabiliti dalla legge e dai regolamenti.

Art. 16 – Trattamenti consentiti

1. L'Azienda, di norma, non è tenuta a chiedere il consenso al trattamento dei dati da parte degli interessati.
2. La pubblicazione e la divulgazione di atti e documenti che determinano una "diffusione e comunicazione" dei dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di individui diversi dall'interessato, è legittima solo se la diffusione è prevista da una norma di legge o di regolamento.
3. Prima della pubblicazione di dati personali deve essere valutato se le finalità di trasparenza e di comunicazione possano essere perseguite senza divulgare dati personali.
4. I dati personali, se possibile, dovranno essere menzionati solo negli atti a disposizione degli uffici, richiamati quale presupposto della deliberazione e consultabili solo da interessati e contro interessati.
5. Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.
6. Per attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione del consenso al trattamento.
7. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Art. 17 – Trattamento dei dati particolari (ex sensibili)

1. Per l'accesso ai dati particolari, con determinazione del Dirigente responsabile, sono rilasciate autorizzazioni singole o a gruppi di lavoro per il trattamento dei dati e la manutenzione.
2. L'autorizzazione è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni assegnate all'incaricato.
3. I dati sensibili individuati dal presente Regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.
4. I dati particolari non indispensabili, dei quali l'Azienda, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato, comunque, non a richiesta dell'organizzazione medesima, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.
5. E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
6. Il divieto di cui al precedente comma non si applica se si verifica uno dei casi definiti dal Regolamento UE art.9 paragrafo 2.

7. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, 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, 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.
8. Fermo quanto previsto dal comma 3, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:
   - accesso a documenti amministrativi e accesso civico;
   - tenuta di registri pubblici relativi a beni immobili o mobili;
   - cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
   - elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
   - esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
   - svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
   - attività di controllo e ispettive;
   - concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
   - rapporti con gli enti del terzo settore;
   - attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
   - rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
   - attività socio-assistenziali a tutela dei minori e soggetti bisognosi non autosufficienti e incapaci.

Art. 18 – Trattamento dei dati Giudiziari

1. Per l'accesso ai dati giudiziari, con determinazione del Dirigente responsabile, sono rilasciate autorizzazioni singole o a gruppi di lavoro per il trattamento dei dati e la manutenzione.
2. L'autorizzazione è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni assegnate all'incaricato.
3. I dati giudiziari sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.
4. I dati giudiziari non indispensabili, dei quali l' Azienda, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato, comunque, non a richiesta dell'Azienda medesima, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.
5. 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, del GDPR deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto europeo o nazione che preveda garanzie appropriate per i diritti e le libertà degli interessati.
6. Fermo quanto previsto dal comma 5, 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. n.101/2018 art 2-octies comma 2.

Art. 19 - Principio di necessità

1. 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, di regolamento o su consenso dell'interessato.
2. I sistemi informativi ed i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estratti degli atti con l'esclusione dei dati personali in essi contenuti.

Art. 20 - Principio di proporzionalità

1. Se la valutazione preliminare porta a constare 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 dell'Azienda, deve essere rispettato il principio di proporzionalità, verificando se sono pertinenti e non eccedenti rispetto alle finalità perseguite.

Art. 21 - Richiesta di soggetti pubblici

1. In presenza di istanze di soggetti pubblici trovano applicazione le disposizioni di cui all'art. 2-ter del codice della Privacy.
2. Qualsiasi richiesta è preceduta da protocollo d'intesa che contiene, di norma, l'indicazione del titolare e del responsabile della banca dati e delle operazioni di trattamento, nonché le modalità di connessione, di trasferimento e di comunicazione dei dati.

Art. 22 - Richiesta 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 per iscritto 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 responsabile del trattamento valuta che la diffusione e la comunicazione sia legittima in base ad una norma di legge o, nei casi previsti dalla legge, di regolamento e che l'accoglimento dell'istanza non leda i diritti e le libertà fondamentali tutelati dal "Codice in materia di protezione dei dati personali", approvato con D.Lgs. 30 giugno 2003, n.196, e, in particolare, 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, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del Regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. 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.

Art. 23 - Attività amministrativa

1. L'attività amministrativa dell'Azienda 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 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).

3. 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 approvato da questo ente con delibera n.54 del 29/10/2014.
4. 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, attuazione dei principi di protezione dei dati, quali la minimizzazione; integrazione nel trattamento delle necessarie garanzie al fine di soddisfare i requisiti del GDPR.
5. I dati sulla 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, possono 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. 25 - Individuazione delle banche dati, del titolare, dei responsabili e degli autorizzati

1. Le banche dati di cui al precedente art. 3, gestite dall'Azienda corrispondono ai programmi previsti dal sistema informatico in esecuzione di deliberazioni e determinazioni adottate dall'organo competente.
2. L'Azienda è titolare dei trattamenti dei dati personali gestiti dalle proprie articolazioni organizzative e delle banche dati ad esse afferenti.
3. Fanno carico ai responsabili delle banche dati tutti gli adempimenti previsti dal D.Lgs. n.196/2003 e dal Regolamento UE 679/2016 (GDPR), comprese le previste comunicazioni e notificazioni al garante.
4. L'Amministratore Unico può, in ogni momento, con provvedimento motivato, designare un dirigente o funzionario apicale che svolga le funzioni monocratiche del titolare del trattamento.
5. I dirigenti dell'Azienda sono designati come autorizzati del trattamento "R*esponsabili della banca dati*" loro affidata.
6. Nelle designazioni dei dirigenti devono essere tassativamente individuate:
   - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie degli interessati;
   - gli obblighi nei confronti del titolare del trattamento.
7. Qualora un responsabile della banca dati si assenti o sia impedito o sospeso per un prolungato periodo di tempo superiore a trenta giorni l'Amministratore Unico provvede alla sua sostituzione temporanea.
8. Il Responsabile della banca dati garantisce che chiunque agisca sotto la sua responsabilità ed abbia accesso a dati personali, sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia adeguato obbligo legale di riservatezza.
9. Il Responsabile della banca dati deve individuare e assicurare la costante continuità delle seguenti figure, espressamente designate:
   - gli autorizzati al trattamento dei dati personali, ciascuno in relazione ai procedimenti amministrativi singolarmente assegnati, come richiesto dal D.Lgs. n.101/2018, art.2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati);
   - uno o più "incaricati privacy" per ciascuna Unità di Direzione, con il compito di supportare gli autorizzati al trattamento dei dati personali, sia a livello informativo che operativo.
10. Il Responsabile della banca dati deve, altresì, provvedere alla valutazione d'impatto sulla protezione dei dati personali, consultando il DPO 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] Elenco delle

tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n.2016/679.

11. Il Responsabile della banca dati deve, altresì, provvedere:

    a. alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

    b. ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach") nelle modalità previste dall'art.31 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;

    c. a 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 4 al presente Regolamento si approva uno schema di informativa tipo che dovrà essere utilizzato dagli autorizzati al trattamento e dai responsabili delle banche dati e aggiornato in base alle ultime modifiche normative;

    d. a curare l'eventuale raccolta del consenso degli interessati per il trattamento dei dati sensibili qualora il loro trattamento non sia previsto da una specifica norma di legge o di regolamento;

    e. 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 all'Ufficio Trattamento Dati Personali di cui al successivo art. 14 con periodicità annuale o su richiesta di quest'ultimo;

    f. documentare sempre l'attività di adeguamento del proprio settore di appartenenza nella maniera più idonea, trasparente e intellegibile per iscritto.

12. Ogni dipendente dell'Azienda che tratta dati personali, deve essere espressamente designato al trattamento dei dati personali secondo l'art.2-quatordecies del codice della Privacy Italiano come integrato del D.Lgs n.101/2018. L'atto di designazione deve essere notificato al dipendente interessato, il quale non può esimersi dalla sua accettazione e attuazione.

13. L'atto di designazione deve contenere le seguenti informazioni:

    - funzioni e compiti attribuiti dei procedimenti amministrativi per lo svolgimento dei quali è indispensabile il trattamento dei dati personali;
    - le finalità del trattamento;
    - le categorie di dati personali da trattare;
    - le operazioni di trattamento eseguibili, con particolare riferimento alla comunicazione e alla diffusione dei dati sensibili e giudiziari;
    - gli eventuali limiti del trattamento;
    - le misure di sicurezza da adottare da parte degli stessi incaricati.

12. I dipendenti possono essere individuati quali Incaricati del trattamento nominativamente ovvero con riferimento alla categoria di inquadramento o al profilo professionale o alla collocazione nell'organizzazione del servizio o dell'ufficio.

13. I dipendenti incaricati del trattamento operano sotto l'autorità dei Responsabili del trattamento, attenendosi alle istruzioni impartire per iscritto, con particolare riferimento alla custodia degli atti e documenti analogici e digitali contenenti dati personali sensibili e giudiziari e alle relative misure di sicurezza.

14. L'attività degli autorizzati al trattamento in materia di tutela della riservatezza dei dati personali è coordinata dallo staff del DPO.

15. Gli autorizzati del trattamento dei dati rispondono del loro operato direttamente ai responsabili delle banche dati di cui al precedente comma 4.
16. Ogni Unità di Direzione dell'Azienda designa una figura come "incaricato privacy" che fungerà da punto di contatto con il DPO. Gli incaricati privacy vengono a far parte dell'Ufficio Trattamento Dati Personali coordinato dal DPO che svolgerà funzioni di consulenza e audit per l'organizzazione.
17. Vengono approvate con questo Regolamento le istruzioni operative per gli autorizzati al trattamento secondo l'art.5 del GDPR alle quali essi dovranno attentamente attenersi: regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Ente (Allegato 5).

Art. 26 - Trattamento dei dati

1. Le disposizioni del presente Regolamento si applicano, in quanto compatibili, al trattamento dei dati in forma non automatizzata.
2. Nelle ipotesi in cui la legge, lo statuto o il regolamento prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le misure eventualmente necessarie per garantire la riservatezza dei dati personali.
3. E' esclusa la messa a disposizione o la consultazione di dati in blocco e la ricerca per nominativo di tutte le informazioni contenute nella banca dati, senza limiti di procedimento o settore, ad eccezione delle ipotesi di trasferimento di dati se previsto da norma o regolamento.
4. Il divieto di cui al precedente comma 3 non si applica al personale dipendente e delle sue articolazioni organizzative a carattere autonomo, che per ragioni d'ufficio acceda alle informazioni e ai dati stessi.
5. Non è consentito mettere a disposizione o a consultazione dati in blocco, né la ricerca per nominativo, di tutte le informazioni contenute nelle banche dati, senza limiti di procedimento o settore, ad eccezione delle ipotesi di trasferimento di dati ad enti pubblici o associazioni di categoria previste da leggi o da regolamento.

Art. 27 - Sicurezza dei dati – Misure di sicurezza – Verifiche e controlli

1. L'Azienda e ciascun Responsabile del trattamento mettono in atto misure tecnico-informatiche, di concerto con l'ufficio SIA, e organizzative idonee per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure di sicurezza devono assicurare di minimizzare il rischio:
   a) di distruzione o perdita, anche accidentale, dei dati memorizzati e comunque assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
   b) di accesso, non autorizzato, alle banche dati, alla rete e, in generale, ai servizi informatici dell'Azienda;
   c) a tutela dei diritti e libertà degli interessati;

   e prevenire:

   - trattamenti illeciti dei dati non conformi alla legge od ai regolamenti;
   - la cessione o la distribuzione dei dati in caso di cessazione del trattamento.

   Inoltre dovrà essere predisposta una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Le persone autorizzate al trattamento e responsabili delle banche dati, così come individuate nelle designazioni previste dall'art.20 comma 5 garantiscono, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, lo sviluppo delle misure di sicurezza dal D.Lgs. n.196/2003 e dal GDPR
4. Nella gestione dei dati personali con il sistema informatizzato dovrà essere assicurato il puntuale e scrupoloso rispetto di tutte le norme vigenti.
5. Gli stessi responsabili delle banche dati si attiveranno periodicamente con controlli, anche a campione, al fine di garantire la sicurezza delle banche dati e la esattezza e completezza dei dati inseriti.

6. Per il trattamento di dati personali, effettuato con strumenti elettronici, sono da considerate tutte le misure idonee al trattamento partendo sempre e comunque dall'allegato 2 al presente Regolamento e valutando, se necessario con opportuna valutazione di impatto DPIA, nuove misure di sicurezza più idonee alla gestione del rischio del trattamento dati personali in considerazione.
7. 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.
8. Risulterà comunque necessario, sentito l'amministratore di sistema, attuare misure tecniche ed organizzative per la mitigazione del rischio proveniente da vulnerabilità.
9. Sarà necessario stipulare un contratto con una società terza, scelta in base alle proprie competenze professionali, per una valutazione periodica della sicurezza delle "applicazioni web" e delle reti informatiche, di conseguenza i test riguarderanno tutto il sistema informatico. Ad esempio, l'analisi di un portale web inizia testando le diverse funzionalità, per poi concentrarsi sul meccanismo di autenticazione e l'interazione con i database. Segue l'analisi della configurazione del relativo server e tutti gli elementi che lo circondano nella rete, e quindi tutti i dati e le informazioni di proprietà di una organizzazione (*Penetration Test*).
10. Il contratto di chi effettua il *Pen Test*, come da articolo precedente, deve presentare clausole di riservatezza, gli indirizzi IP da cui partiranno i test, le persone fisiche responsabili e operative durante l'attività, e l'eventuale collaborazione con operatori e amministratori interni.
11. Colui che effettua un *Pen Test* di un sistema deve garantire la non interruzione delle attività e processi, la non modifica e perdita dei dati e informazioni. Tutte le attività non regolamentate dal contratto sono considerate illegali.
12. Ogni persona autorizzata al trattamento:
    - dovrà preoccuparsi di non utilizzare o divulgare informazioni personali per scopi diversi da quelli per cui sono state raccolte, salvo con il consenso dell'individuo o come richiesto dalla legge;
    - documentare qualsiasi nuovo scopo per la raccolto delle informazioni personali;
    - conservare le informazioni personali solo per il tempo necessario allo scopo;
    - distruggere, cancellare o rendere anonime le informazioni personali che non sono più necessarie per soddisfare gli scopi identificati o se lo prevede la norma;
    - sviluppare linee guida e implementare procedure in relazione alla conservazione delle informazioni personali.
13. Al fine di garantire la sicurezza delle informazioni personali, andranno implementate le seguenti misure organizzative:
    - autorizzazione e limitazione dell'accesso solo alle persone autorizzate (in base alle designazioni);
    - autorizzazione delle persone autorizzate dopo averle istruite e formate, l'accesso alle informazioni sensibili dipenderà dallo status della persona a cui è concesso;
    - accordi di riservatezza e responsabilizzazione mediante le designazioni dei responsabili esterni;
    - specifiche procedure di sicurezza che garantiscano sia la sicurezza dei dati che delle informazioni personali (piano di continuità operativa, di *Disaster recovery*, regolamento sui dati informatici ecc.…);
    - formazione alla sicurezza delle informazioni;
    - regolare monitoraggio interno dei sistemi di sicurezza delle informazioni (*Audit*);
    - monitoraggio e audit regolari e indipendenti dei sistemi di sicurezza delle informazioni.

Dovranno essere inoltre implementate le seguenti misure tecnologiche:

- requisiti di identificazione per stabilire se un individuo è legittimato all'accesso alle informazioni personali;
- autenticazione diversa a seconda della sensibilità delle informazioni (vale a dire, password o altri

identificatori univoci per garantire l'accesso autorizzato alle informazioni personali);

- controlli di accesso al sistema;
- canali sicuri per la trasmissione di informazioni personali;
- crittografia di dati sensibili per l'archiviazione e la trasmissione;
- firewall, sistemi e procedure di rilevamento delle intrusioni;
- audit automatici per i sistemi di elaborazione delle informazioni personali;
- controlli di manutenzione della sicurezza del sistema compresi i *logs*;
- registri e procedure per incidenti di sicurezza.

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

Art. 28 – Best Practices

1. Rientrano tra le *best practices* dell'Azienda:

a. esaminare quali informazioni sono disponibili nella propria organizzazione per determinare se tutte le informazioni personali sono state raccolte per scopi specifici e se è ancora necessario conservare queste informazioni;

b. conservare le informazioni personali solo nei luoghi individuati o comunque inventariare sempre un nuovo archivio informatico o cartaceo;

c. effettuare verifiche periodiche o controlli a campione per garantire che le informazioni personali vengano conservate con misure di sicurezza idonee al trattamento, alla probabilità di rischio, al tipo di informazioni contenute, alla sensibilità delle informazioni personali, la quantità e i tipi di informazioni detenute, come vengono trasmessi e a quante persone, in quali formati;

d. per evitare divulgazioni improprie, stabilire metodi sicuri per distruggere le informazioni non più necessarie (ad esempio, distruggere file cartacei o eliminare in modo sicuro i record elettronici). Considerare, ad esempio, i rischi associati allo smaltimento di computer o stampanti in cui le informazioni personali sono state lasciate sul disco rigido;

e. obbligare mediante contratti sottoscritti con atti vincolanti i responsabili esterni a conservare i dati solo per il periodo necessario e comunque a rispettare le norme vigenti in tema di protezione dati personali;

f. non condividere mai le informazioni personali con alcun individuo o sito Web a meno che la divulgazione sia prevista per norma e per regolamento;

g. se il software di sicurezza del computer visualizza un avviso di sicurezza, prestare attenzione e chiamare l'amministratore di sistema;

h. non collegare le unità USB al computer a meno che non se ne conosca la provenienza, i precedenti collegamenti e solo se strettamente necessario;

i. utilizzare le email e gli indirizzi email in maniera idonea;

j. per evitare le truffe via email, tenere sempre presente l'indirizzo da cui viene inviata l'email;

k. ogni applicazione web prodotta e utilizzata per i servizi di questa Azienda che richiede dati personali, deve utilizzare il protocollo "*https://*" e richiederlo nella barra di navigazione;

l. prestare particolare attenzione quando si tratta di bambini o categorie protette;

m. conservare i dati personali cartacei in schedari o armadi chiusi a chiave dove l'accesso è consentito solo alle persone autorizzate;

n. *clean-desk*: la necessità di non lasciare, soprattutto a fine giornata lavorativa, documenti contenenti dati personali e particolare sulla scrivania o comunque alla vista di altre persone non autorizzate;

o. accesso limitato alle informazioni personali e ai luoghi di lavoro solo alle persone autorizzate o su sorveglianza;

p. garantire che le protezioni fisiche e hardware siano sufficienti a proteggere da perdita o furto e da accesso, divulgazione, copia, utilizzo e modifica non autorizzati;

q. garantire la responsabilità della sicurezza dei dati: i vari tipi di dati personali dovrebbero essere classificati in modo che sia i lavoratori che i dirigenti capiscano le differenze. Classificando i dati personali, i dipendenti dovrebbero essere a conoscenza di come gestire ciascun tipo e quali tipi sono autorizzati a condividere o diffondere;

r. applicare policy ai servizi web e di rete (si stabilisce come si dovrebbero gestire problemi come l'accesso remoto e la gestione e la configurazione degli indirizzi IP e le politiche di rilevamento delle intrusioni);

s. scansione per le vulnerabilità. È importante trovare eventuali vulnerabilità nell'infrastruttura IT prima degli hacker. Poiché gli hacker analizzeranno le vulnerabilità nel momento stesso in cui vengono scoperte, si dovrebbe avere una routine per controllare regolarmente le proprie reti;

t. gestione delle patch: aggiornamenti continui dei sistemi software di base e non;

u. avere politiche condivise di gestione e protezione dei firewall, database e antivirus;

v. la risposta agli incidenti: se si verifica una violazione della sicurezza, è importante disporre di misure appropriate per gestirla immediatamente. Ciò include la valutazione e la segnalazione dell'incidente e il modo in cui risolvere i problemi che ne derivano per evitare il ripetersi del problema;

w. utilizzo accettabile: i dipendenti dovrebbero avere una politica di utilizzo corretto dei dati e dei sistemi ed è buona prassi fare firmare una politica di utilizzo;

x. monitoraggio della conformità: attivare audit interni ed esterni servono a garantire che l'azienda rispetti i vari elementi di politica di sicurezza dei dati. I controlli vanno eseguiti regolarmente;

y. monitoraggio e controllo degli account: gestione e monitoraggio degli accessi ai dati personali. Eliminazione degli account sospesi di persone che erano autorizzate al trattamento. La politica di sicurezza dovrebbe designare specifici membri del team per monitorare e controllare attentamente gli account utente, il che impedirebbe il verificarsi di attività illegale;

z. segmentazione dei dati e della rete.

Art. 29 – Rischio per i diritti e le libertà degli interessati

1. Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e sui diritti degli interessati.
2. Rispetto a tali possibili impatti negativi, il titolare o un suo delegato del trattamento è tenuto a promuovere e adottare approcci e politiche che tengano conto costantemente del rischio, effettuando una analisi attraverso un apposito processo di valutazione (si vedano artt. 35-36 GDPR) che sappia tenere conto:

   - dei rischi noti o evidenziabili;

   - delle misure tecniche e organizzative adottate o che si intende adottare per mitigare il rischio.

3. A tale fine, il titolare o un suo delegato del trattamento, attraverso il sistema di protezione, promuove e adotta approcci e politiche che tengano conto costantemente del rischio, introducendo:

   - l'obbligo di effettuare valutazioni di impatto (DPIA) prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, e di consultare l'Autorità di protezione dei dati in caso di dubbi;
   - adeguate misure di sicurezza;
   - un sistema di monitoraggio sull'efficacia delle misure.

Art. 30 – Valutazione di impatto sulla protezione dei dati personali (DPIA)

1. E' necessario redigere 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. 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;*
3. 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.
4. L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati in capo ai "Responsabili delle Banche Dati", con il coordinamento dell'Ufficio Protezione Dati Personali e dell'Amministratore di Sistema, si applica alle operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.
5. Le valutazioni d'impatto sulla protezione dei dati andranno riesaminate con regolarità, almeno una volta l'anno o quando se ne presenti la necessità dagli stessi soggetti preposti alla redazione con il supporto del DPO.
6. Spetta al titolare del trattamento assicurare che la valutazione d'impatto sulla protezione dei dati sia eseguita.
7. Il Titolare del trattamento deve consultarsi con il DPO, e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, devono essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve altresì sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati (articolo 39, paragrafo 1, lettera c).
8. Il DPO 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.
9. L'Ufficio Trattamento Dati Personali e l'Amministratore di Sistema possono proporre al titolare di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
10. 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.
11. 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;

12. 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.

13. 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.

14. 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.

15. E' pubblicata sul sito istituzionale dell'Azienda, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 31 – Notifica delle 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 ben noti della sicurezza delle informazioni:
   - "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
   - "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
   - 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 il cui schema è adottato come Allegato 6 a questo Regolamento.
4. Il Titolare del trattamento deve 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 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.

5. Il Titolare del trattamento, tramite i responsabili delle banche dati, 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.
6. Il Responsabile del trattamento informi il Titolare del trattamento, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
7. Il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le liberta delle persone fisiche, salve le eccezioni previste dall'art. 34 par. 3 GDPR.
8. Il "Piano di protezione dei dati personali e gestione del rischio di violazione", da redigere con cadenza annuale o biennale da parte dell'Ufficio Protezione Dati Personali con il coordinamento del DPO 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.
9. Le istruzioni operative per la risoluzione delle violazioni dei dati personali e l'eventuali comunicazione all'Autorità Garante e/o agli interessati sono descritte nell'Allegato 4 al presente Regolamento.

Art. 32 - Diritti dell'interessato

1. Ai soggetti di cui questa Azienda tratta dati personali, sono riconosciuti, senza indugio, i seguenti:
   - Diritti di natura "conoscitiva":
     a. (art.13 e 14) ricevere informazione coincisa, semplice e chiara, facilmente intellegibile e accessibile;
     b. (art.15) richiedere/ottenere informazione sul trattamento e sui dati trattati (diritto di accesso);
     c. (art.34) venire a conoscenza su gravi violazione dei propri dati personali.
   - Diritti di "controllo":
     a. (art.6.1.a e 9.2.a) diritto al consenso cioè quello di autorizzare il trattamento;
     b. (art.18) diritto alla limitazione del trattamento cioè modificare il trattamento;
     c. (art.7.3) diritto di revoca del consenso e quindi di far cessare il trattamento;
     d. (art.21) diritto di opposizione e quindi di far cessare il trattamento.
   - Diritti degli interessati che hanno ad oggetto i propri dati personali sono:
     a. (art.20) diritto alla portabilità che è quella di spostare dati complessi e strutturati anche a diverso titolare del trattamento;
     b. (art.16) diritto di rettifica e integrazione che riguarda la possibilità di modificare i dati;
     c. (art.17) diritto all'oblio/cancellazione cioè il diritto di eliminare i propri dati personali
   - Diritto sancito all'art.22 di non subire decisioni unicamente basate su trattamenti automatizzati.
2. L'interessato può esercitare tali diritti con una richiesta senza formalità al responsabile della banca dati o al soggetto autorizzato al trattamento.
3. I soggetti autorizzati devono notificare la richiesta fatta dagli interessati al dirigente e se ritenuto necessario al DPO.
4. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.
5. 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. tutela del segreto.

Art. 33 – Procedure per la risposta ai reclami o richieste riguardante le politiche o le pratiche relative alla gestione dei dati personali.

1. In qualunque momento i cittadini possono far valere i diritti previsti dagli art 15 e successivi del Regolamento generale sulla protezione dei dati 679/2016.
2. Al fine di facilitare l'esercizio dei diritti dell'interessato in materia di protezione dati personali si approva come Allegato 3 il modulo per l'accesso ai dati personali che viene pubblicato sul sito istituzionale nella sezione Amministrazione trasparente e nella sezione privacy.
3. Ogni Responsabile della banca dati dovrà adottare le misure idonee a far conoscere il modello Allegato 3 a tutti gli autorizzati al trattamento al fine di rendere più efficace la comunicazione per gli interessati.

Art. 30 - Entrata in vigore del regolamento

Il presente Regolamento entra in vigore il primo giorno della sua adozione con delibera dell'Amministratore Unico p.t..

Art. 31 - Casi non previsti dal presente Regolamento

Per quanto non previsto nel presente regolamento trovano applicazione: a) le leggi nazionali e regionali; b) lo statuto dell'Azienda, c) il Regolamento aziendale sull'organizzazione generale degli uffici.

Art. 32 - Rinvio dinamico

1. Le norme del presente Regolamento si intendono modificate per effetto di sopravvenute norme vincolanti statali e regionali.
2. In tali casi, in attesa della formale modificazione del presente Regolamento, si applica la normativa sovraordinata.

Art. 33 - Norme abrogate

1. Con l'entrata in vigore del presente regolamento sono abrogate tutte le norme regolamentari con esso contrastanti.

Art. 34 - Pubblicità del regolamento

1. Il presente Regolamento è pubblicato nell'apposita sezione di Amministrazione trasparente del sito internet istituzionale.
2. Il Regolamento è comunicato tramite posta elettronica al Collegio Sindacale e al Responsabile della protezione dei dati personali.

Art. 35 – Modalità di aggiornamento

1. L'adozione del Regolamento non si configura come un'attività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione.
2. Eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi, sono oggetto di approvazione da parte dell'Amministratore Unico p.t..