CITTA' DI SAN BENEDETTO DEL TRONTO
PROVINCIA DI ASCOLI PICENO

Regolamento sulla protezione e libera circolazione dei dati personali ai sensi del Regolamento Generale Protezione Dati (UE) 2016/679 "GDPR"

Approvato con delibera di G.C. n. …….

CAPO I - DISPOSIZIONI GENERALI

Art. 1. - Oggetto

1. Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal Titolare nonché misure procedimentali e regole di dettaglio, nel rispetto di quanto previsto dal Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "GDPR", Regolamento Generale Protezione Dati), dal Codice in materia di dati personali (D.Lgs. n. 196/2003) aggiornato dal D.Lgs. n. 101/2018 s.m.i., dalle Linee guida e raccomandazioni del Garante e dalle Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29), nonché dell'European Data Protection Board (EDPB) applicabili.
2. Il presente Regolamento individua i soggetti mediante i quali il Comune di San Benedetto del Tronto esercita le funzioni di Titolare del trattamento dei dati personali, i loro ruoli e responsabilità.
3. Le disposizioni del presente Regolamento si applicano a tutte le articolazioni organizzative del Comune di San Benedetto del Tronto.

Art. 2. - Definizioni

1. Il presente regolamento si avvale delle seguenti definizioni:
   - Per "*Codice*", il Codice in materia di protezione dei dati personali introdotto con il decreto legislativo 30 giugno 2003, n. 196, modificato e integrato con il Decreto Legislativo 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle Disposizioni del Regolamento UE 2016/679" e dal D.L. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla L. 3 dicembre 2021, n. 205 recante "Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali";
   - per "*Regolamento*" il "Regolamento UE 2016/679" ("GDPR") 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";
   - per "*trattamento*", qualunque operazione o complesso di operazioni, svolti con l'ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione di dati personali;
   - per "*dato personale*", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, nonché i dati rilevati con trattamenti di immagini effettuati mediante gli impianti di videosorveglianza;
   - per "*dato personale comune*": qualsiasi informazione riguardante una persona fisica (interessato), identificata o identificabile. 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 di caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
   - per "*dati personali particolari*": c.d. "sensibili", ovvero i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i 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.
   - per "*dati giudiziari*": i dati personali idonei a rivelare condanne penali, reati o connesse misure di sicurezza, oltre che i provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o

la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

- per *"Titolare del trattamento dei dati personali"* o anche "Titolare", il Comune di San Benedetto del Tronto, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali. Al Titolare, anche unitamente ad altro Titolare, spettano le decisioni in ordine alle modalità del trattamento e agli strumenti utilizzati. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa in materia di protezione dei dati personali.
- per *"Responsabile del trattamento dei dati personali"* o anche "Responsabile", la persona fisica o giuridica, individuata dal Titolare, a cui viene esternalizzata un'attività o un servizio che richiede connesse operazioni di trattamento di dati personali per conto del Titolare. I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione europea o degli Stati membri.
- per "*Responsabile della protezione dei dati"* o "D.P.O.", si intende il soggetto nominato dal Titolare del trattamento, che affianca il medesimo nella gestione delle pratiche relative al trattamento dei dati. In particolare, il DPO ("Data Protection Officer") ha il compito di informare il Titolare ed i responsabili, nonché i soggetti autorizzati, circa gli obblighi previsti in materia di privacy; se richiesto, fornire parere al Titolare in merito alla valutazione d'impatto dei trattamenti sulla protezione dei dati e sorvegliare i relativi adempimenti; cooperare con le autorità di controllo; fungere da punto di contatto con i soggetti interessati in merito a qualsiasi problematica dovesse emergere riguardo ai trattamenti dei dati; consultare l'autorità di controllo anche di propria iniziativa;
- per *"autorizzati"*, chiunque, sia esso definito "Designato" o "Incaricato", agisce sotto l'autorità del Titolare o del Responsabile che abbia accesso e gestisca dati personali per le funzioni che gli competono;
- per *"designati"*, coloro che operano sotto l'autorità del Titolare e sono stati individuati da questi a svolgere specifici compiti e funzioni di primo livello connessi al trattamento di dati personali;
- per *"incaricati"*, coloro che operano sotto l'autorità del Titolare e svolgono compiti di secondo livello in merito al trattamento dei dati personali;
- per "*amministratore di sistema"*, si intende il personale sistemistico e di networking, che ha facoltà di accesso alle informazioni anche senza i vincoli e le protezioni del livello applicativo;
- per "*interessato"*, la persona fisica a cui si riferiscono i dati personali;
- per "*pseudonimizzazione"*: il trattamento di dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
- per "*Garante"*: l'autorità pubblica di controllo indipendente di cui agli artt. 2-bis e 153 e ss. Del Codice, istituita dalla legge 31 dicembre 1996, n. 675, per vigilare sulla corretta applicazione della normativa in materia di protezione dei dati personali.

Art. 3. - Finalità del trattamento

1. Il Titolare garantisce che il trattamento dei dati personali, a tutela delle persone fisiche, si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'integrità, alla disponibilità delle informazioni personali e dell'identità personale a prescindere dalla loro nazionalità o della loro residenza.

2. Il Titolare, nell'ambito delle sue attribuzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.
3. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi di competenza del Titolare sono gestiti conformemente alle disposizioni del Codice, del GDPR e del presente Regolamento.

Art. 4. - Principi e responsabilizzazione

1. Vengono integralmente recepiti, nell'ordinamento interno del Titolare, i principi del GDPR, per effetto dei quali dati personali sono:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
   b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("limitazione della finalità");
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati base del principio di "minimizzazione dei dati";
   d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati base del principio di "esattezza";
   e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "limitazione della conservazione";
   f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di "integrità e riservatezza";
   g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità ("principio di necessità").
2. Il Titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione" (o accountability).

Art. 5. - Liceità del trattamento dei dati personali comuni

1. Vengono integralmente recepiti, nell'ordinamento interno del Titolare, le disposizioni del GDPR in ordine alla liceità del trattamento dei dati personali comuni e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
   a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
   b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) non si applica al trattamento di dati effettuato dal Titolare nell'esecuzione dei propri compiti e funzioni.

Art. 6. - Liceità del trattamento dei dati personali particolari

1. Il Titolare si conforma a quanto previsto dall'art. 9 GDPR che disciplina il trattamento di categorie particolari di dati personali. Nello specifico il GDPR sancisce il divieto di 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.
2. Nel paragrafo successivo l'art. 9 GPDR individua le circostanze in cui tale divieto non si applica:
   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
   e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
   g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (nel rispetto di quanto previsto all'art. 2-sexies Codice Privacy);
   h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo;
   i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o

la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 7. - Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
2. 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. 8. - Informativa

1. Il Titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale Incaricato, apposita informativa secondo le modalità previste dagli artt. 13 e 14 del GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
2. L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.
3. L'informativa è fornita, mediante idonei strumenti:
   a) attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
   b) avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del Titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante apposita pubblicazione sulla sezione dedicata del sito istituzionale;
   c) apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Titolare;
   d) resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'Incaricato del trattamento dei dati relativi alle procedure, anche tramite diciture brevi richiamanti informative più ampie.
4. L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto.
5. L'informativa contiene il seguente contenuto minimo:
   a) l'identità e i dati di contatto del Titolare e, ove presente, del suo rappresentante;

b) i dati di contatto del D.P.O.;
c) le finalità del trattamento;
d) i destinatari dei dati;
e) la base giuridica del trattamento;
f) l'interesse legittimo del Titolare se quest'ultimo costituisce la base giuridica del trattamento;
g) se il Titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
h) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
i) il diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
j) il diritto di presentare un reclamo all'autorità di controllo;
k) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

6. Nel caso di dati personali non raccolti direttamente presso l'interessato:
   a) il Titolare deve informare l'interessato anche in merito a:
   - le categorie di dati personali trattati;
   - la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;
   b) l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.
7. Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del Titolare è predisposta apposita informativa per personale dipendente.
8. Nel fornire l'informativa, il Titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari. È prevista la possibilità di fornire informative "brevi" che richiamino informative più estese.

Art. 9. - Sensibilizzazione e formazione

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della protezione dei dati, e migliorare la qualità del servizio.
2. A tale riguardo, Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento anche eventualmente integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.
3. La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione dell'accountability dell'Ente.

Art. 10. - Trattamento dei dati del personale

1. Il Titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo, nel rispetto degli obblighi di legge.

2. Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.
3. Secondo la normativa vigente, il Titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.
4. Il trattamento dei dati sensibili del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.
5. La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici. Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.
6. Il Titolare, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.
7. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

CAPO II - DIRITTI DEGLI INTERESSATI

Art. 11. - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio e/o l'area amministrazione trasparente, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:
    a) sicurezza
    b) completezza
    c) esattezza
    d) accessibilità
    e) minimizzazione
    f) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.
2. Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati o pseudonimizzati, tranne deroghe previste da specifiche disposizioni.
3. Salva diversa disposizione di legge, il Titolare garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on line o sulla rete civica, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il Titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.
4. Il Titolare si conforma alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

Art. 12. - Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

1. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati sensibili e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
2. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
3. Il Titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Art. 13. - Diritti dell'interessato

1. Il Titolare deve garantire ed agevolare, nel rispetto della normativa vigente, l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea.
2. Il Titolare si impegna a non utilizzare i dati che, a seguito di verifiche, dovessero risultare eccedenti o non pertinenti o non necessari. Per garantire un trattamento di dati corretto e trasparente, l'interessato ha diritto di chiedere al Titolare:
   - Diritto di accesso: accedere ai propri dati e conoscere chi vi ha avuto accesso (art. 15 GDPR);
   - Diritto di rettifica: richiedere l'aggiornamento, la rettifica o l'integrazione dei dati (art. 16 GDPR);
   - Diritto alla cancellazione e di limitazione: richiedere la cancellazione («diritto all'oblio») e la limitazione del trattamento se trattati in difformità dalla legge, fatti salvi gli obblighi legali di conservazione (artt. 17 e 18 GDPR);
   - Diritto alla portabilità: ricevere, nei casi normativamente previsti, in formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un Titolare del trattamento unitamente al diritto di trasmettere (se possibile) tali dati ad un altro Titolare, senza impedimenti da parte del Titolare del trattamento cui li ha forniti, qualora:
     - il trattamento si basi sul consenso ai sensi dell'art. 6 GDPR, o dell'art. 9 GDPR o su un contratto ai sensi dell'art. 6 GDPR;
     - il trattamento sia effettuato con mezzi automatizzati (art.20 GDPR);

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

   - Diritto di opposizione: opporsi, per motivi legittimi, al trattamento dei dati (art. 21 GDPR).
3. Ai sensi dell'art. 77 GDPR, resta impregiudicato per l'interessato il suo diritto, qualora ne ricorrano le condizioni, di rivolgere reclamo al Garante per la Protezione dei Dati Personali secondo le modalità indicate sul sito www.garanteprivacy.it .
4. Ogni diritto deve essere valutato anche nel rispetto dei limiti indicati dagli artt. 23 GDPR, 2-undecies e 2-duodecies Codice Privacy.
5. Il modulo per esercitare i diritti in materia di protezione dei dati è pubblicato sul sito istituzionale, nell'apposita sezione, oppure presso gli uffici.

Art. 14. - Modalità di esercizio dei diritti dell'interessato

1. Per l'esercizio dei diritti dell'interessato si applicano le disposizioni del GDPR, del Codice, del presente Regolamento e della relativa procedura, di seguito descritta.
2. La richiesta per l'esercizio dei diritti può essere fatta pervenire:

- direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;
- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;
- tramite chi esercita la responsabilità o la tutela, per i minori e gli incapaci;
- in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
- dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.

3. L'interessato può presentare o inviare la richiesta di esercizio dei diritti:
   - all'ufficio del Protocollo generale del Titolare;
   - all'indirizzo e-mail del DPO presente sul sito Istituzionale nella sezione dedicata.
4. La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento:
   - alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.
5. Fermo restando l'accesso ai dati personali, il dirigente autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.
6. I soggetti competenti alla valutazione dell'istanza sono:
   - il dirigente competente;
   - il Responsabile per la protezione dei dati (D.P.O.);

che decidono sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.

7. All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo. L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del Titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.
8. Il Titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

CAPO III – SOGGETTI

Art. 15. - Titolare del trattamento

1. Il Comune di San Benedetto del Trono, rappresentato ai fini previsti dal GDPR dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").
2. Il Titolare nomina il Responsabile della protezione dei dati (di seguito DPO) tra i soggetti in possesso dei requisiti previsti dal GDPR e stabilisce la durata dell'incarico. Della nomina dà comunicazione al Garante per la Protezione dei Dati Personali e alle strutture interessate.
3. In conformità all'assetto organizzativo del Titolare, i soggetti individuati, ciascuno per il rispettivo ambito di competenza, quali autorizzati al trattamento sono distinguibili in due categorie:

a) Soggetti Designati al trattamento (Dirigenti)
b) Soggetti Incaricati al trattamento (tutti gli altri dipendenti).

4. I soggetti di cui sopra sono responsabili del rispetto dei principi applicabili al trattamento dei dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.
5. Inoltre, gli stessi soggetti sono tenuti a porre in essere, nell'ambito delle Aree e Servizi di competenza, ove necessario anche in collaborazione con quanto predisposto e indicato dal Servizio informatica, misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.
6. Le misure sono definite 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 e ss. GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Art. 16. - Soggetti autorizzati al trattamento

I soggetti autorizzati al trattamento dei dati personali si suddividono in:

a) DESIGNATI

Con il presente Regolamento si individuano quali designati al trattamento dei dati, in ragione e nei limiti del loro mandato, le seguenti figure:

- Il Segretario Generale, nell'ambito dei trattamenti effettuati negli Uffici/ Servizi allo stesso sottoposti;
- I Dirigenti, nell'ambito dei trattamenti effettuati nella relativa Area/ Settore.

Queste figure sono i riferimenti del Titolare, il quale, con il presente Regolamento, impartisce a essi le necessarie istruzioni in relazione alle informative agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati e all'eventuale uso di apparecchiature di videosorveglianza.
Con il presente Regolamento gli stessi sono informati delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice e dal GDPR.
I Designati, in ossequio al GDPR, devono attenersi alle seguenti istruzioni:

a) verificare la legittimità dei trattamenti di dati personali effettuati dall'Area/ Settore di riferimento;
b) presidiare l'aggiornamento dei registri delle attività di trattamento e il monitoraggio dei rischi per la relativa direzione di competenza, comunicando eventuali eventi potenzialmente dannosi per gli interessati;
c) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13-14 del GDPR;
d) individuare i responsabili esterni e i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento e, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
e) predisporre ogni adempimento organizzativo necessario per gestire le procedure che garantiscano agli interessati l'esercizio dei diritti previsti dalla normativa;
f) collaborare con il Responsabile per la protezione dei dati al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
g) garantire al Responsabile per la protezione dei dati i necessari permessi di accesso ai dati e ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

Nell'attuazione dei compiti sopra indicati i soggetti sopra individuati possono contattare e acquisire il parere del DPO.

Ciascun Designato, nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il Titolare al fine di:

- comunicare tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio;
- informare il Titolare, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali,
- collaborare nella notificazione di una violazione dei dati personali al Garante privacy, nella comunicazione di una violazione dei dati personali all'interessato, nella redazione della valutazione d'impatto sulla protezione dei dati o nell'eventuale consultazione preventiva.

Ciascun Designato risponde al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.
I Designati sono destinatari degli interventi di formazione e di aggiornamento.

b) INCARICATI

Con il presente Regolamento si stabilisce che il personale dipendente del Titolare, i tirocinanti, i collaboratori continuativi e/o altri soggetti, eventualmente anche individuati dai dirigenti, che comunque operano sotto l'autorità del Titolare, sono autorizzati, in relazione ai compiti loro conferiti, al trattamento dei dati personali nel rispetto delle mansioni ricoperte e nei limiti delle finalità connesse al rapporto di lavoro con l'Ente, coerentemente con quanto previsto dalle norme vigenti e dal presente Regolamento. Gli incaricati collaborano con il Titolare ed il dirigente/Designato segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
Per effetto di tale disposizione, ogni dipendente e collaboratore a qualsiasi titolo tenuto ad effettuare operazioni di trattamento è da considerare autorizzato ai sensi dell'art. 2-quaterdecies del Codice nonché ai sensi degli artt. 4 co.10 e art. 29 del GDPR.
Tali soggetti, possono essere formalmente autorizzati:

1. tramite individuazione nominativa (nome e cognome) delle persone fisiche.
2. tramite assegnazione funzionale della persona fisica alla unità organizzativa/Direzione/ Area.

Nel primo caso, l'autorizzazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento. Tali istruzioni devono contenere un espresso richiamo al presente Regolamento e alle policy in materia di sicurezza informatica e protezione dei dati personali.
Nel secondo caso, con il presente Regolamento si impartiscono a essi le seguenti istruzioni, anche in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza:
- gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:

- trattati solo nell'ambito delle funzioni ricoperte e dell'attività regolarmente assegnatagli;
- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- trattati con la riservatezza, l'integrità e la disponibilità che la segretezza dell'ufficio richiede;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

- gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal dirigente, nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del Titolare.

Gli incaricati dipendenti del Titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 17. - Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

1. Il presente Regolamento, approvato con specifica Delibera di Giunta del Titolare, costituisce a tutti gli effetti di legge un regolamento comunale che il personale dipendente dell'ente deve osservare rigorosamente a pena di comminazione di sanzioni disciplinari così come previste dal Codice disciplinare comunale (pubblicato ai sensi del D.lgs. n. 150/2009) e della Contrattazione Collettiva nazionale relativa al pubblico impiego.
2. Ad ogni modo, ai fini del presente Regolamento si evidenzia che il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è punito con le sanzioni previste dagli articoli da 166 a 172 del Codice Privacy da parte dell'Autorità di controllo oltre alle sanzioni di natura disciplinare sopra richiamate.
3. Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento con conseguente violazione del presente Regolamento.
4. Il Responsabile del trattamento risponde per il danno causato dal trattamento solamente se non abbia adempiuto agli obblighi previsti dal Codice, dal GDPR e dal presente Regolamento e allo stesso specificamente diretti o qualora abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare.
5. Il Titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 18. - Responsabile del trattamento (RDT) e sub responsabili

1. Il Responsabile è il soggetto che, in ragione di un rapporto giuridico, svolge attività di trattamento dei dati per conto del Titolare.
2. Il Responsabile è nominato dal Titolare. In particolare, il Titolare può avvalersi per il trattamento di dati, anche sensibili/particolari, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Se nominato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario.
4. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-Responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento

dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-Responsabile.

5. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.
6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede a:
   - trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia;
   - rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
   - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
   - ad individuare per iscritto le persone, soggette alla propria autorità e vigilanza, autorizzate al trattamento dei dati personali e dare loro le istruzioni idonee per il trattamento dei dati personali;
   - a conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli e al Titolare su richiesta del medesimo;
   - ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
   - ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;
   - trattare i dati personali, anche di natura sensibile, del Titolare esclusivamente per le finalità previste dal contratto o dalla convenzione;
   - attenersi alle disposizioni impartite dal Titolare del trattamento;
   - specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;
   - comunicare le misure di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
8. In caso di mancato rispetto delle precedenti disposizioni e di mancata comunicazione al Titolare dell'atto di nomina dei soggetti autorizzati al trattamento, laddove richiesti, risponde direttamente il Responsabile del trattamento nei confronti del Titolare. La nomina del Responsabile viene effettuata mediante atto da parte del Titolare del trattamento da allegare agli accordi, alle convenzioni o ai contratti che prevedono l'affidamento a soggetti esterni di trattamenti di dati personali.
9. L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento sono condizioni necessarie per l'instaurazione del rapporto giuridico fra le parti

Art. 19. - Amministratori di Sistema

1. L' Amministratore di sistema sovraintende alla gestione e alla manutenzione delle banche dati e nel suo complesso, al sistema informatico di cui è dotata l'amministrazione.
2. La nomina dell'Amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto individuato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di

sicurezza. La designazione dell'Amministratore di sistema è individuale e nominativa e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

3. L'Amministratore di sistema svolge le attività quali il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.
4. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'Amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
5. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo non inferiore ai 6 mesi.
6. Secondo la normativa vigente, l'operato dell'Amministratore di sistema deve essere verificato con cadenza annuale da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.
7. Il Titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
8. L'Amministratore di sistema è destinatario degli interventi di formazione e di aggiornamento.

Art. 20. - Responsabile della protezione dati "DPO"

1. Il Responsabile della protezione dei dati (DPO) è individuato anche all'esterno, come azienda o professionista, tramite procedura ad evidenza pubblica, fra soggetti aventi idonee qualità professionali, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili.
2. I compiti attribuiti al DPO sono indicati in apposito contratto di servizio che richiama i seguenti punti:
   a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
   b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
   d) cooperare con l'autorità di controllo;
   e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
3. Il Titolare ed i Designati 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/P.O. che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
   - il DPO deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio, ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione;
- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. 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;
   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 Designato.
5. La figura del 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 per la trasparenza;
   - il Responsabile del trattamento;
   - qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
6. Il Titolare e i Designati forniscono al DPO le risorse necessarie per assolvere i compiti attribuiti e garantiscono l'accesso ai dati personali ed ai trattamenti. In particolare, è assicurato al DPO:
   - supporto attivo per lo svolgimento dei suoi compiti;
   - tempo sufficiente per l'espletamento dei compiti affidati al DPO;
   - supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione);
   - comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
   - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
7. Il 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.
8. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare - Sindaco o suo delegato - o ai Designati.
9. 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 Designato.
10. Il DPO non può essere rimosso o penalizzato dal Titolare e dal Designato per l'adempimento dei propri compiti.

CAPO IV SICUREZZA DEI DATI PERSONALI

Art. 21. - Misure di sicurezza

1. L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.
2. Il Comune di San Benedetto del Tronto mette in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio tenendo conto 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.

3. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico, una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
4. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun autorizzato:
   - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
   - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici;
   - altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
5. Il Comune di San Benedetto del Tronto si impegna ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi ed i dati di contatto del Titolare, e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Titolare.

Art. 22. - Registro delle attività di trattamento

1. Il Titolare del trattamento istituisce un registro, anche in formato digitale, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità nel rispetto dell'art. 30 GDPR.
2. Il Registro delle attività di trattamento svolte dal Titolare reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del Comune e del DPO;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.
3. Il Titolare, per il tramite di ciascun soggetto dallo stesso Designato ai sensi del precedente art. 4, conserva presso gli uffici della struttura organizzativa del Titolare il Registro.
4. Ciascun Designato ha la responsabilità della regolare tenuta e aggiornamento del Registro delle attività di trattamento con riferimento agli ambiti di competenza.
5. Qualora l'organizzazione svolga l'attività di trattamento in qualità di Responsabile esterno, adotta il registro delle attività di trattamento svolte per conto di un Titolare.

Art. 23. - Valutazioni d'impatto sulla protezione dei dati

1. La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
2. La DPIA è uno strumento importante per la responsabilizzazione del Titolare in quanto consente allo stesso non soltanto di rispettare i requisiti previsti dal GDPR ma anche di dimostrare che sono state adottate misure appropriate per garantire il rispetto dello stesso.
3. La DPIA sulla protezione dei dati personali deve essere realizzata prima di procedere al trattamento dal Titolare quando un tipo di trattamento, consideratane la natura, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Per

"rischio" si intende uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità e per "gestione dei rischi" l'insieme delle attività coordinate al fine di indirizzare e controllare un'organizzazione.

4. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, GDPR.
5. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
   d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, GDPR;
   e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
   f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
   g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
   h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
   i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

6. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Titolare. Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA. Ciascun Designato deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il Responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.
7. 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. Il Responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi,

possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

8. La DPIA non è necessaria nei casi seguenti:
   - ✓ se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, GDPR;
   - ✓ se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   - ✓ se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy e che proseguano con le stesse modalità oggetto di tale verifica. Le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

9. 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. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
   b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
      - delle finalità specifiche, esplicite e legittime;
      - della liceità del trattamento;
      - dei dati adeguati, pertinenti e limitati a quanto necessario;
      - del periodo limitato di conservazione;
      - delle informazioni fornite agli interessati;
      - del diritto di accesso e portabilità dei dati;
      - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
      - dei rapporti con i responsabili del trattamento;
      - delle garanzie per i trasferimenti internazionali di dati;
      - consultazione preventiva del Garante privacy;
   c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
   d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.
11. Il Titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il Responsabile della protezione dei dati personali. Laddove la DPIA riveli la presenza di rischi residui elevati, il Titolare è tenuto a richiedere la consultazione preventiva dell'Autorità di controllo in relazione al trattamento ai sensi dell'art. 36, paragrafo 1 GDPR.

Art. 24. - Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la

divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Titolare.

2. Ogni dipendente che venga a conoscenza di una violazione dei dati personali è tenuto a segnalarlo, direttamente o per il tramite del proprio referente, tempestivamente al Titolare del trattamento e al DPO.
3. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, sentito il parere del DPO, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.
4. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:
   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti, discriminazione;
   - furto o usurpazione d'identità;
   - perdite finanziarie, danno economico o sociale;
   - decifratura non autorizzata della pseudonimizzazione;
   - pregiudizio alla reputazione;
   - perdita di riservatezza dei dati personali protetti da segreto professionale.
5. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, "senza ingiustificato ritardo", con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie particolari di dati personali;
   - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   - comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
   - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio, utenti deboli, minori, soggetti indagati).
6. La notifica deve avere il contenuto minimo previsto dall'art. 33 GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
7. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

Art. 25. - Procedura in caso di accertamento ispettivo o richieste istruttorie da parte dell'Autorità

1. L'attività ispettiva e ogni ulteriore richiesta da parte dell'Autorità garante richiede una cooperazione totale tra Titolare, DPO e Autorità stessa. In ragione di ciò, laddove dovesse pervenire una richiesta da parte dell'Autorità o ci fosse un'attività ispettiva, è necessario che il Titolare sia pronto a rispondere a ogni richiesta nel rispetto del principio dell'accountability, che fonda l'intera struttura del GDPR. A tal fine, la presente procedura stabilisce un "Gruppo di risposta" composto dal Dirigente della Direzione/Area eventualmente interessata, dal Segretario generale, dal Responsabile della protezione dei dati e, se necessario, da un referente dell'Area che gestisce i sistemi informativi.

2. La presenza del Responsabile della protezione dei dati (DPO) è necessaria e fondamentale anche per fare da intermediario tra il Titolare e l'Autorità. Pertanto, dovrà essere convocato subito e, se assolutamente impossibilitato per ragioni oggettive, laddove non si possa posticipare l'incombente, lo stesso potrà individuare un suo idoneo sostituto.

Art. 26. - Regole di comportamento con riguardo alla protezione dei dati personali

1. Trattare un dato personale vuol dire compiere qualunque operazione o complesso di operazioni con o senza l'ausilio di strumenti elettronici. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo i principi generali a tutela della privacy, che possono essere considerati vincoli inscindibili al trattamento dei dati personali.
2. Si stabiliscono, pertanto, le regole relative alla:
    a. gestione dei locali e delle risorse fisiche

a.1. Tutti i locali e tutte le risorse fisiche del Titolare devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un elevato livello di sicurezza delle informazioni.
a.2. L'accesso agli uffici, alle aree riservate e agli archivi cartacei è permesso agli utenti autorizzati muniti di badge personale o cartellino identificativo, in base a precise e motivate esigenze lavorative.
a.3. I visitatori e gli ospiti di vario tipo potranno avere accesso agli uffici comunali esclusivamente dietro autorizzazione.
a.4. L'accesso ai locali del Data Center è permesso esclusivamente a personale autorizzato munito della relativa chiave o codice di apertura porta e, in via eccezionale, agli addetti al controllo e alla manutenzione dello stesso opportunamente accompagnati dal personale interno competente.

    b. gestione della postazione di lavoro e dei dati in generale

b.1. L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.
b.2. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati disponibili all'accesso di terzi in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.
b.3. I documenti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere. I documenti devono essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.
b.4. I documenti e gli atti contenenti dati particolari devono essere custoditi in armadi chiusi a chiave.
b.5. L'eliminazione fisica di ogni documento cartaceo o supporto informatico contenente dati e informazioni istituzionali e/o personali deve essere effettuata solo utilizzando appositi e idonei strumenti e modalità.
b.6. Si raccomanda di non lasciare documenti incustoditi presso i dispositivi di stampa e di distruggere personalmente le stampe quando non servono più.
b.7. Ogni utente è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi adottare ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità e il corretto utilizzo.
b.8. I dati e le informazioni possono essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le modalità connesse alla propria attività lavorativa.
b.9. È vietata la comunicazione di dati e di informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e alla efficacia ed efficienza dell'attività dell'Ente o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.
b.10. È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

b.11. La diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.
b.12. In caso di furto o smarrimento di fascicoli o atti contenenti dati personali l'utente deve informare immediatamente per iscritto il proprio Responsabile di Servizio ed il Dirigente. Dovrà altresì informare il Responsabile Protezione Dati.

c. degli strumenti informatici

c.1. Per la gestione degli strumenti informatici si fa riferimento a quanto stabilito dal Regolamento per l'utilizzo degli strumenti informatici e dalle singole procedure IT ad esso allegate.

Art. 27. - Rinvio

1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.
2. Il presente Regolamento si considera automaticamente aggiornato nei casi di modifiche ed integrazioni normative in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari della Direzione Generale si intendono immediatamente recepiti nel presente Regolamento.

Art. 28 - Abrogazione

Con l'entrata in vigore del presente Regolamento sono abrogati il "Regolamento comunale per l'attuazione del regolamento U.E. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali" e il "Regolamento sulla tutela della riservatezza dei dati personali contenuti in archivi e banche dati del Comune di San Benedetto del Tronto" approvato con delibera del Commissario straordinario n. 169 del 18/05/2006.