OGGETTO: Indirizzi e linee guida di adattamento al Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Adattamento dell'organizzazione alle disposizioni contenute nel Regolamento UE 2016/679.

Art. 1 - Oggetto

1. le presenti linee guida hanno per oggetto misure procedimentali e indirizzi di adattamento ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data ProtectionRegulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Bisceglie.

Art. 2 - Finalità del trattamento

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

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

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

b) l'adempimento di un obbligo legale al quale è soggetto l'Ente;

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

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

La base su cui si fonda il trattamento dei dati di cui alla lett. a) e b) è stabilita dalla fonte normativa che lo disciplina.

Art. 3 - Mappatura dei processi

1. Nell'ottica di creare un sistema comunale di data protector si procederà alla puntuale mappatura dei processi:

- per individuare quelli collegati al trattamento dei dati personali;
- per definire un ordine di priorità, previa individuazione dei processi che presentano rischi;
- per definire eventuali proposte di miglioramento dei processi.

Art. 4 – Titolare del Trattamento

1. Il Comune di Bisceglie, rappresentato ai fini previsti dal RGPD 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 è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

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

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

6. Il Titolare, inoltre, provvede a:

a) designare i Responsabili "interni" del trattamento nelle persone dei Dirigenti di Settore in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

b) designare gli amministratori del Sistema Informativo Comunale;

b) demandare, previa relativa designazione, ai Responsabili "interni" del trattamento, la formalizzazione del contratto da cui scaturiscono gli obblighi ex art. 28 paragrafo 3 del RGPD a carico dei Responsabili "esterni" del trattamento, ossia dei soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

c) designare il Responsabile della protezione dei dati;

d) predisporre l'elenco dei Responsabili del trattamento interni/esterni in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

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

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

Art. 5 – Responsabili "interni" del Trattamento.

1. In relazione alle dimensioni organizzative del Comune, sono designati Responsabili "interni" del Trattamento i Dirigenti dei Settori in cui si articola l'organizzazione comunale, in quanto in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le

misure tecniche e organizzative volte a garantire che i trattamenti siano effettuati in conformità al RGPD.

2. I Responsabili "interni" del trattamento dei dati provvedono, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti loro affidati dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvedono:

- a collaborare alla gestione del registro delle attività di trattamento del Comune come da successivo art. 12;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- collaborare alle richieste di accesso, di limitazione ed opposizione degli interessati relative a trattamenti di dati personali;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- 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.

3. I Responsabili "interni" del trattamento, sono designati, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;

- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

- gli obblighi ed i diritti del Titolare del trattamento.

4. I Responsabili "interni" del trattamento, possono altresì designare altri soggetti incaricati, identificandoli nei Titolari di P.O. e nei Responsabili di Servizio, ciascuno per il proprio ambito operativo.

Art. 6 – Responsabili esterni del Trattamento

1. I Responsabili esterni del trattamento sono le persone fisiche, giuridiche, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo esterno all'Amministrazione comunale che, previa designazione formale dei Responsabili "interni" del trattamento, assumono (su delega di questi ultimi)

poteri decisionali su un determinato trattamento e devono attenersi, nelle operazioni svolte, alle istruzioni ricevute.
2. Detti soggetti, in qualità di responsabili del trattamento, devono fornire le garanzie di cui al precedente art. 4 comma 1 e stipulare atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
3. Gli atti di cui innanzi devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

Art. 7 – Amministratore di Sistema

1. L'Amministratore di Sistema è, in ambito informatico, la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software, le reti locali e gli apparati di sicurezza, nella misura in cui tali attività di gestione e manutenzione consentano di intervenire sui dati personali.
2. Il Titolare, per l'effetto di quanto indicato al precedente comma 2 provvederà alla designazione formale degli Amministratori di Sistema.

Art. 8 – Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "DPO") è individuato previa ricognizione "interna", fra i dipendenti del Comune di qualifica non inferiore alla cat. D, purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il DPO mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
2. Ove la ricognizione "interna" abbia esito sfavorevole si procederà tramite procedura ad evidenza pubblica o altra procedura di affidamento nei limiti consentiti dalla vigente normativa; i compiti attribuiti al DPO sono indicati in apposito contratto di servizi. Il DPO esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento.

3. E’ possibile l’affidamento dell’incarico di DPO ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267.
4. Il DPO è incaricato dei seguenti compiti:
   - 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 regolamento nonché da altre disposizioni dell'Unione o nazionali relative alla protezione dei dati;
   - vigilare sull'osservanza del Regolamento e delle altre disposizioni dell'Unione o nazionali relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   - fornire, se richiesto, parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;
   - cooperare con l'autorità Garante per la protezione dei dati personali;
   - fungere da punto di contatto per l'autorità Garante per la protezione dei dati personali per questioni connesse al trattamento, tra le quali la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
   - tenere il registro delle attività di trattamento sotto la responsabilità del titolare o dei responsabili del trattamento stesso, atteso quanto previsto dalle “linee guida sui responsabili della protezione dei dati” del gruppo di lavoro articolo 29 per la protezione dei dati adottate il 13 dicembre 2016 e successivamente emendate e adottate in data 5 aprile 2017, con riferimento all'art. 39, paragrafo 1;
   - definire un ordine di priorità nell’attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati, consentendo allo stesso di consigliare più facilmente al titolare quale metodologia seguire nel condurre una DPIA, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo. Tanto, in considerazione di quanto previsto dalle “linee guida sui responsabili della protezione dei dati” del gruppo di lavoro articolo 29 per la protezione dei dati adottate il 13 dicembre 2016 e successivamente emendate e adottate in data 5 aprile 2017, con riferimento all'art. 39, paragrafo 2.
5. La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili (in relazione alle dimensioni organizzative del Comune):

- 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 si impegna ad assicurare le risorse finanziarie occorrenti all'adeguamento della struttura agli obblighi rivenienti dal GDPR nonché alle indicazioni del DPO. Il Titolare assicura, altresì, al DPO:
   - tempo sufficiente per l'espletamento dei compiti affidati al medesimo;
   - supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione) e, ove richiesto, personale;
   - 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. Il DPO non può essere rimosso o penalizzato dal Titolare e dai Responsabili del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare (in persona del Sindaco o suo delegato) o ai Responsabili del trattamento. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed ai Responsabili del trattamento.

Art. 9 – Gruppo di Lavoro GDPR

1. A supporto del DPO ed al fine di perseguire l'obiettivo del completo adeguamento alle norme del GDPR, è istituito un gruppo di lavoro permanente composto da:
   - segretario comunale (coordinatore);
   - dirigenti dei settori, in qualità di responsabili "interni" del trattamento;
   - soggetti incaricati del trattamento, così come indicati al precedente art. 4 comma 4;
   - almeno un referente del servizio ICT, quale amministratore di sistema, per le problematiche di sicurezza tecnologica.

2. Il gruppo di lavoro definisce ed aggiorna in particolare:

- la mappatura dei processi, così come definita al precedente art. 3;
- un programma permanente di informazione e formazione del personale

- le priorità di intervento per l'adattamento al GDPR
- le misure da adottare per il rispetto della normativa
- la modulistica uniforme sia ad uso esterno che ad uso interno (informativa, consenso, comunicazioni, registri ecc...)
- la redazione e l'aggiornamento dell'elenco dei responsabili e dei designati.

Art. 10 - Sicurezza del trattamento

1. Il Comune di Bisceglie e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

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

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Settore cui è preposto ciascun Responsabile del trattamento:

- 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.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. 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.

6. Il Comune di Bisceglie e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

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

8. 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. 11 – Responsabilizzazione

1. Il titolare ed i designati assicurano in ogni momento il rispetto dei principi previsti dal GDPR (art. 5) dettando le opportune disposizioni organizzative e procedurali in ogni fase dell'attività, assicurando in particolare il rispetto del principio di responsabilizzazione nell'attuazione delle disposizioni del GDPR.

Art. 12 – Registro delle attività di trattamento

1. Il Responsabile della Protezione dei Dati con il supporto informativo del Gruppo di lavoro, previa adozione del relativo modello, cura l'aggiornamento del registro delle attività di trattamento di cui all'art. 30 del GDPR, mediante acquisizione dai responsabili dei servizi dei dati e delle informazioni necessarie.

2. Il registro è aggiornato tempestivamente in occasione della variazione dei trattamenti e comunque almeno una volta ogni 12 mesi.

3. Il registro, depurato di eventuali informazioni non necessarie o che possano mettere a rischio la sicurezza dell'Ente è pubblicato sul sito internet nella sezione dedicata al GDPR.

Art. 13 - Principio di collaborazione

1. Tutto il personale coinvolto nelle procedure di trattamento dati, a qualunque livello e ruolo:

- collabora con il titolare, il DPO, l'autorità di controllo ed eventuali ulteriori soggetti addetti alla vigilanza, controllo ed attuazione delle disposizioni in materia di trattamento dei dati fornendo la massima e tempestiva collaborazione con particolare riferimento al rispetto dei principi previsti dal GDPR;

- fornisce tempestivamente informazioni su potenziali pericoli, rischi, o violazioni dei dati personali anche al fine di consentire l'esercizio dei compiti di cui all'art. 33 e 34 del GDPR (cosiddetto "data breach");

- collabora con i responsabili del trattamento, al fine di garantire le citate finalità e nel rispetto degli obblighi di segretezza e riservatezza;

2. Il rispetto dei principi in materia e dei compiti ed adempimenti previsti dal presente provvedimento verrà valutato in sede di raggiungimento degli obiettivi e/o negli altri casi di responsabilità del personale a vario titolo coinvolto.

Art. 14 – Rinvio

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