COMUNE DI BORGHETTO SANTO SPIRITO
(Provincia di Savona)

Servizio Affari Generali

Allegato "A"

Piano di protezione e modello organizzativo a tutela dei dati personali

Attività	*Atto*	*Organo*	*N.ro*	*Data*	*Esecutività*
Approvazione	Delibera	Giunta Comunale	0	0	0

Sommario

PREMESSA

Il 25 maggio 2018 è divenuto ufficialmente applicabile il nuovo Regolamento generale in materia di Protezione dei Dati personali entrato in vigore il 24 maggio 2016. Il GDPR, acronimo di "General Data Protection Regulation" va ad abrogare, dopo oltre un ventennio, la cosiddetta direttiva madre n. 95/46/C, che, fino ad oggi, costituiva il quadro normativo di riferimento a livello europeo.
Il nuovo Regolamento costituisce, insieme alla Direttiva (UE) n. 2016/680, il "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea.
Il Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 fa riferimento a dati concernenti persone identificate o identificabili in possesso di vari soggetti e quindi anche della Pubblica Amministrazione utilizzabili per le proprie finalità istituzionali. Dati che devono essere trattati nei limiti delle funzioni dell'ente, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.

L'apparato normativo si regge su di un nuovo principio di fondamentale importanza: la responsabilizzazione, ovvero il principio di *accountability* (nell'accezione inglese la cd. "responsabilizzazione"): tale concetto rappresenta un'assoluta novità nel campo della protezione dei dati personali, in quanto il titolare del trattamento, oltre ad avere l'esclusiva competenza per il rispetto dei principi e delle regole previste dal GDPR, deve anche essere in grado di comprovarne il corretto adempimento.

Ai titolari, altresì, viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative ed alla luce di alcuni criteri indicati dal regolamento.

Come specifica chiaramente l'art. 25 del GDPR, uno di quei criteri è sicuramente rappresentato dall'espressione anglofona "*data protection by default and by design*" ossia dalla necessità di configurare il trattamento prevedendo dall'inizio, ovvero fin dalla fase di progettazione, le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Spetta dunque al titolare mettere in atto una serie di misure tecniche ed organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.

Tra le nuove attività previste dal GDPR, riguardo agli obblighi dei titolari, saranno fondamentali quelle relative alla valutazione del rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio da impatti negativi sulle libertà e sui diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per diminuirne l'impatto.

Una lettura organica e sistematica del Regolamento europeo consente di affermare che, data l'importanza della normativa e di ciò che essa mira a proteggere, la migliore risposta in termini di cambiamento organizzativo sia quella di realizzare un complessivo "Modello organizzativo e di gestione" per la protezione dei dati personali, considerando come tale un complesso di attività organizzativa, di ruoli, di azioni organizzative, di sistemi mirato al fine dell'applicazione "ordinata" e completa, nell'azione amministrativa dell'Ente, della normativa sui trattamenti di dati personali. Tale logica di costruzione di un Modello *ad hoc* è, peraltro, simile a quella risultante, in materia di prevenzione della corruzione.

L'adeguamento al Regolamento UE 2016/679 impone al titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, tale Modello organizzativo individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle

libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche, logiche, logistiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Al fine di garantire la migliore e più puntuale attuazione del principio di accountability, il presente modello organizzativo contiene disposizioni regolamentari che costituiscono la base minima indefettibile la cui concreta attuazione è demandata all'organizzazione del personale operante all'interno dell'Ente, nelle sue articolazioni gerarchiche.

Il presente modello organizzativo sarà sottoposto a revisione ogni qualvolta si renderà necessario.

PARTE I - NORME E PRINCIPI GENERALI

Questa Amministrazione assicura che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.
In attuazione del suddetto principio il Comune assicura che, nello svolgimento dei compiti e funzioni istituzionali, i dati personali siano trattati nel rispetto della legislazione vigente oltre che dei seguenti principi:

a) «liceità, correttezza e trasparenza»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) «limitazione delle finalità»: i dati personali sono 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, conformemente all'art. 89, prf. 1, del RGDP, considerato incompatibile con le finalità iniziali;
c) «minimizzazione dei dati»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) «necessità»: è ridotta 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;
e) «esattezza»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
f) «limitazione della conservazione»: i dati personali sono 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'art. 89, prf. 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato;
g) «integrità e riservatezza»: i dati personali sono 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;
h) «responsabilizzazione»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo.

SENSIBILIZZAZIONE E FORMAZIONE

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma soprattutto, come garanzia per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.
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 Comune sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.
A tale riguardo, questa Amministrazione riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale nonché quella diretta a tutti coloro che hanno rapporti con il Comune.
Per garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio, è data ad ogni dipendente una specifica comunicazione, con apposita clausola inserita nel

contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente Modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie. Per lo stesso motivo, ad approvazione avvenuta del presente documento, copia dello stesso è notificata/consegnata, anche tramite studenti informatici, a tutto il personale dipendente già in servizio.
Il Comune organizza, anche in collaborazione con il DPO, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di aggiornamento 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.
La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Comune.
La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

TRATTAMENTO DEI DATI PERSONALI
Il Comune tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali, quali identificate da disposizioni di legge, statutarie e regolamentari, e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo.
Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati ed autorizzati secondo quanto previsto infra nel presente documento.
Non è consentito il trattamento da parte di persone non puntualmente autorizzate, anch' esse siano gestori di servizi etc., ed istruite in tal senso.
Al fine di garantire la correttezza delle operazioni di trattamento provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti svolti, finalizzata alla compilazione ed aggiornamento del Registro delle attività di trattamento di cui al GDPR.

Tipologie di dati trattati
Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali, il Comune tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati personali, quali definiti all'articolo 4, paragrafo 1, del GDPR;
- categorie particolari di dati personali di cui all'art. 9, paragrafo 1, del GDPR (c.d. dati sensibili);
- categorie particolari di dati personali di cui all'art. 2-septies del D.Lgs. 196/2003 (c.d. dati super-sensibili);
- dati personali relativi a condanne penali e reati di cui all'articolo 10 del GDPR (c.d. dati giudiziari).

Trattamento dei dati relativi a condanne penali e reati
Il titolare conforma il trattamento dei dati giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato ed è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati. Sono inoltre autorizzati i trattamenti individuati con apposito Decreto del Ministero di Giustizia, (così come previsto dal D. Lgs. 101/2018), riguardanti condanne penali, reati o misure di sicurezza per:

a) l'adempimento di obblighi e l'esercizio di diritti in materia di lavoro nei limiti stabiliti da leggi, regolamenti e contratti collettivi;
b) l'adempimento di obblighi in materia di mediazione per la conciliazione di controversie civili e commerciali;
c) la verifica dei requisiti di onorabilità, requisiti soggettivi e presupposti interdettivi;
d) l'accertamento della responsabilità in relazione a sinistri, nonché la prevenzione di frodi;
e) l'accertamento l'esercizio e la difesa di diritto in sede giudiziaria;
f) l'esercizio dei diritti di accesso a dati e documenti nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;

g) l'esecuzione di investigazioni o ricerche o raccolta di informazioni presso terzi ai sensi dell'art. 134 del testo unico delle leggi di pubblica sicurezza;
h) l'adempimento di obblighi in materia di comunicazioni e informazioni antimafia o per la produzione della documentazione prescritta per partecipare a gare d'appalto;
i) l'accertamento dei requisiti di idoneità morale di coloro che intendono partecipare a gare di appalto, in adempimento della normativa in materia di appalti;
j) l'attuazione della disciplina del rating di legalità delle imprese;
k) l'adempimento degli obblighi previsti dalla normativa antiriciclaggio.

Il Decreto del Ministero della Giustizia autorizza il trattamento dei dati effettuato in attuazione dei protocolli di intesa per la prevenzione ed il contrasto della criminalità organizzata di concerto con il Ministero dell'Interno e le Prefetture UTG. Il Titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati particolari e giudiziari. I dati personali trattati in violazione della disciplina in materia di trattamento non possono essere utilizzati salvo quanto previsto dall' art 160 bis del Codice relativamente all'uso nei procedimenti giudiziari.

Trattamento dei dati particolari relativi alla salute

Il titolare si conforma alle misure di garanzia disposte dal Garante con cadenza biennale in materia di trattamento dei dati personali particolari relativi allo stato di salute, ai dati genetici e biometrici che non possono essere diffusi, con particolare riferimento ai contrassegni sui veicoli e gli accessi alle zone a traffico limitato di cui al Decreto del Ministero delle Infrastrutture e della mobilità sostenibile del 05 luglio 2021, che ha istituito la Piattaforma unica nazionale informatica dei contrassegni unici (CUDE).

I dati idonei a rivelare lo stato di salute sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

Trattamento dei dati del personale

Il titolare tratta i dati, anche di natura particolare 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. 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. 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.

Il trattamento dei dati particolari 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 particolari, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

Il trattamento dei dati presenti nei curricula spontaneamente trasmessi non necessita di consenso.

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.

Il Titolare, nel trattamento dei dati particolari relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità. 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.

Finalità del trattamento

Il Comune effettua periodicamente una ricognizione delle finalità che impongono o consentono il trattamento dei dati personali, anche sensibili (e super-sensibili) e giudiziari.

In sede di prima stesura del presente documento, viene predisposto apposito elenco (a carattere esemplificativo e non esaustivo) contenente le principali finalità del trattamento (vedi allegato "1") .

CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizioni normative che lo vietino, il Comune favorisce la circolazione all'interno dei propri uffici dei dati personali dei cittadini il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del GDPR.

La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti.

Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati da predetti articoli 9 e 10 del GDPR.

COORDINAMENTO DI NORME

L'Amministrazione intende perseguire l'obiettivo di assicurare le forme più estese di accessibilità e trasparenza sul proprio operato ad opera dei cittadini, nelle varie forme in cui il diritto di accesso è riconosciuto, quali (a titolo esemplificativo) quella prevista dal TUEL (D.Lgs. 267/2000) negli articoli 10 e 43, quella prevista dalla Legge 241/90 e quella prevista dal D.Lgs. 33/2013 e ss.mm.ii..

A tale proposito - fermo restando che 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 e la relativa tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione restano disciplinati dalla normativa di settore – gli uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto (eventualmente, in caso di accesso) controinteressato.

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigente, l'ufficio, nel dare riscontro alle richieste di accesso ovvero nel pubblicare i provvedimenti, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei «dati personali» in esso presenti, laddove l'esigenza informativa, alla base dell'accesso o della trasparenza e pubblicazione, possa essere raggiunta senza implicare il trattamento dei dati personali.

In merito, vedasi anche l'apposito paragrafo "Accesso civico generalizzato e protezione dati personali".

PARTE II - PROFILO ORGANIZZATIVO

PROFILO STRUTTURALE

La prima risposta organizzativa è l'individuazione di una struttura organizzativa per la protezione dei dati personali, che, ovviamente, si sovrapponga, in gran parte, all'attuale struttura amministrativa dell'Ente, integrandosi con essa. La creazione di tale struttura, comporta tre azioni principali:

- il disegno di struttura (organigramma) per la Privacy;
- la definizione dei ruoli;
- l'individuazione dei soggetti "abilitati" dall'Ente a trattare i dati personali.

Conseguente, alla costruzione, sarà quindi necessario adeguare le competenze mediante la formazione e informazione dei soggetti, abilitando concretamente i soggetti stessi.

Struttura competente

Spetta al Servizio Affari Generali, per il tramite dell'U.O. Società partecipate - Amm.ne trasparente - Privacy - Attività legge 150/2000 l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario; svolge, altresì, un ruolo di supporto al DPO in tema di risorse strumentali e di competenze. La struttura è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di *accountability*, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al GDPR da parte del DPO.
In particolare

- individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente; tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del DPO, come, ad esempio, la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e l'aggiornamento dei disciplinari tecnici trasversali;
- condivide le evidenze dell'analisi dei rischi con il DPO, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;
- provvede, ogni qualvolta venga avvertito un problema di sicurezza, tenuto altresì conto di quanto previsto dal GDPR e dalle regolamentazioni adottate dall'Ente, a:
  - ✓ attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;
  - ✓ individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO;
  - ✓ segnalare tempestivamente al DPO le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;
- svolge verifiche sulla puntuale osservanza della normativa e delle policy di Ente in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dello stesso;
- promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno dell'Ente, coordinandosi con le azioni promosse dal DPO.

  Al TPO competente in materia spetta:
- la sottoscrizione degli atti di notifica e di consultazione preventiva al Garante;
- la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

IL TITOLARE DEL TRATTAMENTO

L'art. 4 paragrafo 7 del GDPR precisa che il titolare del trattamento (interpretando la norma rispetto all'Ente locale) è "*l'autorità pubblica*" che "*determina le finalità e i mezzi del trattamento di dati personali*".
Il concetto di Titolare del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:

a) determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);
b) mettere in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. *accountability*) (art. 24);
c) garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
d) individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
e) agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
f) designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
g) istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
h) effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
i) comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
j) ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
k) rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
l) rispondere delle violazioni amministrative ai sensi del GDPR (art. 83).

Alla luce del testo normativo e delle interpretazioni correnti, si ritiene che titolare sia l'Ente locale nel suo complesso in quanto la legislazione nazionale gli ha affidato il compito di raccogliere e trattare certi dati personali. Tuttavia, in concreto, esso manifesta la propria volontà attraverso coloro a cui è attribuito il potere di decidere per l'Ente, nell'ambito delle suddivisioni di ruolo nascenti dal diritto amministrativo.
Le competenze e le responsabilità quali delineate dal GDPR e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi del Comune in relazione alle funzioni agli stessi assegnati dal D.Lgs. n. 267/2000 e ss.mm.ii e dallo Statuto comunale. Tale ripartizione è così intesa da questa Amministrazione:

A. al Consiglio comunale sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;
B. all'organo esecutivo (Giunta comunale) sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del Consiglio, con particolare riferimento agli atti e attività a contenuto organizzativo e di indirizzo;
C. all'organo di vertice (Sindaco) competono le nomine e le designazioni rilevanti in materia di protezione dei dati personali, con riferimento in particolare al Responsabile della protezione dei dati, ai soggetti designati con funzioni di coordinamento (Responsabili di posizione organizzativa), al Segretario;
D. ai Responsabili di posizione organizzativa, secondo l'ambito di competenza, spettano i seguenti compiti (con elencazione meramente esemplificativa):
    a. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;

b. disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c. adottare soluzioni di privacy by design e by default;
d. contribuire al costante aggiornamento del registro delle attività di trattamento;
e. garantire la corretta informazione e l'esercizio dei diritti degli interessati;
f. individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
g. disporre l'adozione dei provvedimenti imposti dal Garante;
h. collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
i. individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
j. garantire al Responsabile della protezione dei dati personali ed al personale (eventualmente) designato Amministratore di sistema i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
k. la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
l. consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1, lett b), nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 indichi che il trattamento presenta un rischio residuale elevato;
m. gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;
n. individuare i responsabili (esterni) ed i contitolari del trattamento fornendo le necessarie indicazioni.

In base al GDPR, invero, responsabile e titolare hanno compiti e doveri molto simili. È sempre tale testo normativo, del resto, a definire obblighi e responsabilità direttamente applicabili al responsabile privacy. La conformità al GDPR è un obbligo condiviso da titolare e responsabile del trattamento. In particolare i principi dell'art. 5 del GDPR relativi al trattamento dei dati personali si applicano ai Responsabili del trattamento tanto quanto si applicano ai Titolari del trattamento dei dati.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DPO/RPD)

Il Comune si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD o DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.
Esso è designato con decreto del Sindaco. Al fine di garantire continuità del servizio, in caso di variazione del DPO/RPD, la nomina può essere fatta antecedentemente alla scadenza del predecessore, indicando chiaramente la data d'inizio dell'attività. Sino alla designazione del nuovo Responsabile della protezione dei dati si intende prorogato di diritto quello in carica.
Può essere designato un dipendente a tempo indeterminato di questo Comune inquadrato in una categoria non inferiore alla D) qualora in possesso di titoli abilitativi, attestati di specifici corsi e competenze documentabili ovvero un soggetto esterno, persona fisica o soggetto giuridico appositamente qualificato.
L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del RPD.
I dati identificativi e di contatto del DPO sono pubblicati nel sito web istituzionale dell'Ente, rendendoli accessibili da un apposito link, comunicati all'Autorità di controllo, comunicati ai componenti degli organi di governo, a tutti i dirigenti e dipendenti comunali, ai componenti degli organi di controllo

interni nonché sono inclusi in tutte le informative rese agli interessati ai sensi degli articoli 13 e 14 del GDPR.
Il Responsabile della protezione dei dati (RPD) che deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del Titolare del trattamento oppure sulla base di un contratto di servizio.

È tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
Il Titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.
Il RPD svolge i seguenti compiti, nel rispetto del segreto professionale e della riservatezza:

- informa e fornisce consulenze al Titolare del trattamento, nonché formazione ai dipendenti che eseguono il trattamento dei dati, con cadenza almeno annuale, in merito agli obblighi vigenti relativi alla protezione dei dati, estesa altresì all'utilizzo di nuove tecnologie quali, ad esempio, la videosorveglianza, analizza i sistemi informativi e l'impatto delle nuove tecnologie in ambito del trattamento dati al fine di consigliare l'ente nell'adozione delle misure di sicurezza;
- verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
- garantisce risposte istantanee (o comunque non superiori ai termini indicati dal Regolamento europeo 2016/679/UE e dalla normativa in materia) ed un numero illimitato di interventi e risposte afferenti alla materia di propria competenza;
- funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- funge altresì da punto di contatto e cooperare con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunge il principio di accountability che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della *compliance* normativa.

Pareri del DPO

Il Responsabile protezione dati fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano nei casi di seguito indicati.

Pareri obbligatori

Devono essere obbligatoriamente richiesti pareri in ordine a:

- individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di incidenti di sicurezza o analisi dei rischi;
- adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;
- individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- incidenti sicurezza;
- esternalizzazione di servizi e/o in cloud che comportino la trattazione di dati personali.

Pareri facoltativi

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

- progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;

- valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;
- valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis del D.Lgs. 14 marzo 2013, n. 33 e, in via generale, del Regolamento UE n. 679/2016;
- opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere devono essere inviate dall'indirizzo di posta elettronica certificata dell'Ente: **comuneborghettoss@postecert.it** oppure via posta elettronica ordinaria all'indirizzo **comune@comune.borghettosantospirito.sv.it** a mezzo protocollo e per conoscenza al Responsabile di P.O. della U.O. competente in materia privacy e protezione dati.
Possono presentare le richieste di parere i TPO designati relativamente alla disciplina di trattamento dati nelle materie di rispettiva competenza.
I pareri sono espressi nel rispetto delle seguenti codifiche:

- NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;
- OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
- PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri "NC" e "OS" il Titolare di PO deve formalizzare, nelle medesime forme utilizzate dal DPO per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO. I pareri espressi dal DPO sono conservati agli atti del servizio che ne ha fatto richiesta e quella competente in materia di privacy (AA.GG.).

IL REFERENTE DEL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'articolo 38 del GDPR, il Titolare ha l'obbligo di assicurarsi che "*il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*"; il Titolare inoltre sostiene "*il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".
Si ravvisa dunque la possibilità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati - di individuare uno o più dipendenti interni all'Ente cui assegnare il compito di "Referente" al fine di supportare l'attività del Responsabile della Protezione dei dati personali (RPD o DPO), nelle seguenti attività:

a) informazione e consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori best practice in materia di analisi e valutazione dei rischi.
b) sorveglianza dell'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare 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 GDPR. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei software e della relativa documentazione tecnica;

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 prevista dall'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.

Qualora il Referente non sia un titolare di P.O. soggiace, comunque, gerarchicamente, dal Responsabile del servizio nel quale è inquadrato. Questi è tenuto al segreto od alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al RPD ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.
Ove i compiti assegnati al Referente vengano svolti in modo collettivo da parte di un team, dovrà essere designato un soggetto coordinatore.
Spetta al Responsabile del servizio o al Segretario c.le, qualora il dipendente non appartenga al servizio AA.GG., identificare e designare il referente a cui assegnare, oltre a quanto già previsto, anche altri compiti o funzioni.

IL RESPONSABILE DEL TRATTAMENTO

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.
L'esistenza di un Responsabile del trattamento dipende da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità - o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.
A norma dell'art. 28, paragrafo 1, del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".
Per poter agire come Responsabile del trattamento occorrono quindi tre requisiti: essere una persona giuridica distinta dal Titolare, elaborare i dati personali per conto di quest'ultimo ed avere conoscenze approfondite in materia di GDPR.
La liceità dell'attività di trattamento dei dati da parte del Responsabile è determinata dal mandato ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile diventa (con)Titolare.
In linea di massima è automatica l'attribuzione di responsabile ai TPO, ma non deve essere esclusa la possibilità di altre persone in possesso dei requisiti previsti. Si deve tuttavia prendere atto del fatto che esistano situazioni in cui la relazione tra l'Amministrazione comunale ed un altro soggetto, pubblico o privato possa generare dei dubbi in merito alla corretta qualificazione del ruolo soggettivo rivestito (Titolare o Responsabile). Con riferimento a tali fattispecie, questo Ente adotta il criterio della valutazione delle circostanze di fatto, suggerito dal Gruppo ex art. 29 nel Parere 1-2010 (WP 169).
Il paragrafo 3 dell'art. 28 del GDPR prevede che "*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 o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*"; il paragrafo 9, da ultimo, prevede che "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*".
Spetta ai Responsabili di P.O. identificare gli eventuali sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai

responsabili e dagli eventuali sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi, risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni.
Il Responsabile di P.O. competente per materia in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.
La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

IL RESPONSABILE ESTERNO DEL TRATTAMENTO

Il responsabile esterno del trattamento dati viene definito dall'art.28 del GDPR come la persona fisica o giuridica, autorità pubblica o organismo che tratta i dati per conto del Titolare del trattamento e non appartiene giuridicamente a quest'ultimo.
I Responsabili esterni del trattamento dei dati devono assistere i Titolari del trattamento in varie circostanze: ad esempio in una potenziale notifica di violazione dei dati personali o nel prendere in considerazione una valutazione d'impatto sulla protezione dei dati.
Una delle caratteristiche del responsabile del trattamento dati è che l'art. 4 GDPR lo definisce come un soggetto esterno all'Ente. Ne consegue che questo ruolo non può essere svolto da un dipendente. La nomina del Responsabile trattamento dati spetta al Titolare del trattamento.
Qualora l'Ente si avvalga di gestori di servizi esterni, per ciò che riguarda le modalità di individuazione, in sede di avviso pubblico/affidamento diretto l'Ente richiede un'autocertificazione inerente agli standard di accountability perseguiti dal soggetto (*conditio sine qua non* per la stipula dei contratti di affidamento con l'Ente).
Inoltre, occorre citare nel bando di gara che il soggetto aggiudicatario sarà nominato responsabile esterno del trattamento dati personali ex art. 28 del GDPR.
La nomina a responsabile del trattamento ex art 28 GDPR deve essere effettuata *in addendum* rispetto alla contrattualizzazione, come appendice contrattuale e deve essere sottoscritto, per la sua validità, da entrambe le parti contraenti.
Nel contratto inoltre:

- deve essere fatta menzione che allo scadere del termine contrattuale il dato personale oggetti di trattamento potrà o essere distrutto o essere restituito, il tutto reso con apposita certificazione;
- il responsabile esterno ha l'obbligo di comunicare un eventuale sub-responsabile del trattamento. Permane la facoltà del Titolare del trattamento di esprimere il proprio diniego.

Il Titolare non può scegliere casualmente il Responsabile esterno del trattamento dati: l'art. 28 stabilisce che il Titolare del trattamento dati deve assicurarsi di collaborare con Responsabili del trattamento che offrano sufficienti garanzie in merito alla loro effettiva capacità di elaborare i dati personali in linea con il GDPR e la protezione dei diritti dell'interessato.
In altri termini, è onere del Titolare accertarsi che i Responsabili siano figure conformi ai requisiti richiesti dal Regolamento Privacy.
Requisiti essenziali del Responsabile esterno del trattamento dati personali sono:

- essere esterno rispetto all'azienda/Ente;
- avere conoscenze approfondite del GDPR.

I RESPONSABILI DI POSIZIONE ORGANIZZATIVA (P.O.)

Già in attuazione del D.Lgs. n. 196/2003, nel testo previgente all'adeguamento al GDPR, Responsabili di Posizione organizzativa (P.O.) sono stati nominati, come avviene tutt'oggi con nomine in atti, responsabili interni del trattamento dei dati per i trattamenti rientranti nella competenza di ciascuno di essi.
L'art. 28 del GDPR ha definito il Responsabile del trattamento come il soggetto che effettua il trattamento "*per conto del titolare*".

Conformemente alle disposizioni del GDPR e del Codice della privacy nel suo testo vigente, il Titolare ed il Responsabile del trattamento possono quindi designare, sotto la propria responsabilità ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati.
L'Amministrazione ritiene dunque che i Responsabili di Posizione organizzativa (P.O.) debbano conseguentemente essere autorizzati al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione e /o contenuto nel decreto di nomina.
Spetta al Sindaco in qualità di Titolare del trattamento dati designare i responsabili di P.O. a cui assegnare lo svolgimento di specifici compiti e funzioni sulla base di quanto contenuto nel presente documento.
Considerato che ai Titolari di P.O. spetta l'adozione degli atti e provvedimenti amministrativi, compresi tutti gli atti che impegnano l'Amministrazione verso l'esterno, nonché la gestione finanziaria, tecnica ed amministrativa mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo e che essi sono responsabili, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui sono preposti, appare opportuno attribuire loro specifici compiti e funzioni spettanti al Titolare, ferma restando l'imputazione della responsabilità conseguente al trattamento in capo al Titolare medesimo.
In merito vedasi anche le competenze attinenti al registro delle attività di trattamento.

IL SEGRETARIO COMUNALE

L'art. 28 del GDPR ha definito il Responsabile del trattamento come il soggetto che effettua il trattamento "*per conto del titolare*".
Visto il ruolo e le funzioni del Segretario comunale quali definiti nell'articolo 97 del D.Lgs. 18 agosto 2000 n. 267 (TUEL), non risulta configurabile un rapporto di rappresentanza "per conto del titolare".
Questa Amministrazione ritiene dunque che il Segretario comunale, al pari dei responsabili di P.O. che sostituisce ed indipendentemente che sia titolare di P.O. o Responsabile di U.O. debba conseguentemente essere autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità ai paragrafi che precedono.

IL DESIGNATO (O AUTORIZZATO) AL TRATTAMENTO - INCARICATI

Il GDPR non prevede espressamente la figura degli "incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'art. 29, rubricato "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", il quale stabilisce che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";
Il Codice privacy, all'articolo 2-quaterdecies prevede che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".
Il GDPR e la normativa nazionale di adeguamento, consentono dunque di mantenere le funzioni ed i compiti assegnati a figure interne all'Ente che, ai sensi del Codice nel testo previgente all'adeguamento al GDPR, ma non anche ai sensi del GDPR, potevano essere definiti come "incaricati".
Il personale operante (a qualunque titolo ed a qualunque livello) all'interno del Comune è conseguentemente autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al presente modello organizzativo.
Spetta ai Responsabili di P.O. identificare e designare per iscritto ed in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le

persone fisiche della struttura organizzativa medesima, che operano sotto la diretta autorità del Titolare ed attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento,
A tal fine, il Sindaco e i Titolari di P.O. hanno l'onere di impartire analitiche istruzioni e controllare costantemente che le persone fisiche designate, delegate ed autorizzate al trattamento dei dati effettuino le operazioni di trattamento in attuazione dei seguenti principi:

- «liceità, correttezza e trasparenza»;
- «minimizzazione dei dati»;
- «limitazione della finalità»;
- «esattezza»;
- «limitazione della conservazione»;
- «integrità e riservatezza».

L'AMMINISTRATORE DEL SISTEMA INFORMATICO

Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" come modificato con successivo provvedimento datato 25/06/2009, il Comune si avvale di un amministratore del sistema informatico a garanzia che il sistema informatico di questo Ente sia strutturato e gestito in modo da consentire l'attuazione delle misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.
Nell'atto ovvero nel contratto di servizio con cui è designato l'Amministratore di sistema devono essere riportati, altresì, tutti gli adempimenti – con tutto ciò che essi comportano sia sul piano delle procedure amministrative, che dell'organizzazione, che dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali – imposti dalle fonti di diritto europee e nazionali, dal "Gruppo di Lavoro europeo ex art. 29", dal Garante della Privacy, dalle disposizioni regolamentari e dalle direttive emanate dal Titolare del trattamento e dal Responsabile della protezione dei dati, nonché per conformarsi alla disciplina del Codice dell'amministrazione digitale di cui al Decreto legislativo n. 82/2004 e ss.mm.ii., in particolare la cura dei seguenti adempimenti:

a) gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate e quant'altro attinente all'esigenza in essere;
b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema; impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per gli Incaricati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzate;
d) verificare costantemente che il Comune abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo senza indugio agli adeguamenti eventualmente necessari, redigendo entro il 30 settembre di ogni anno una apposita relazione da inviare al Sindaco, al Segretario ed al Responsabile per la protezione dei dati in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure;
e) suggerire al Comune l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati, atte a che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

L'Amministratore di sistema, nominato dal Titolare del trattamento, sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.
Può essere designato un dipendente comunale a tempo indeterminato inquadrato almeno nella categoria "C", in possesso di specifiche competenze documentabili, ovvero, nel caso di mancanza di un dipendente, un soggetto esterno, persona fisica o giuridica.
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. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo rispetto ai trattamenti affidati e comunque non superiore ad un anno.
Secondo la normativa vigente, l'operato dell'Amministratore di sistema deve essere verificato, 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. 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.
Più specificamente, l'Amministratore di sistema dovrà svolgere le funzioni previste in apposito Disciplinare tecnico.
Al soggetto individuato per tale funzione è:

a) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati. Tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Responsabili del trattamento a conoscere i dati personali oggetto di trattamento;
b) obbligato a dare tempestiva comunicazione al Sindaco ed ai Responsabili del trattamento interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;
c) obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.

Il Responsabile della protezione dei dati procederà periodicamente alla verifica delle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

IL CONTITOLARE DEL TRATTAMENTO

In base alla previsione contenuta nell'articolo 26 del GDPR "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*".
In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.

Spetta ai Responsabili di P.O. identificare gli eventuali contitolari di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai contitolari l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni.
Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.
I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali. È tuttavia ammessa una diversa ripartizione "Interna" del profilo di responsabilità, da valutarsi caso per caso.

PARTE III - ADEMPIMENTI E PROCEDURE

MISURE PER LA SICUREZZA DEI DATI PERSONALI

La Giunta comunale, Responsabili di P.O. e l'Amministratore del sistema informatico provvedono, per quanto di rispettiva competenza, all'adozione ed alla dimostrazione di aver adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato 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.
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 di trattamento dati;
- 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.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Ai sensi dell'articolo 30 del GDPR "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*".
La medesima norma individua il contenuto minimo di tale registro, specificando poi che esso è tenuto in forma scritta, anche in formato elettronico e dev'essere messo a disposizione dell'autorità di controllo.
La tenuta di siffatto registro, in forma scritta digitale, si configura pertanto come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal GDPR e non soltanto come strumento operativo di mappatura dei trattamenti effettuati.
Un'altra grande differenza rispetto al D.lgs. 196/2003 è la modalità di mantenimento di tale documento. Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato.
È intenzione del Comune, appena possibile, adottare un sistema informatico che meglio possa consentire l'aggiornamento e l'accesso alle informazioni. Il sistema informatico dovrà rispettare il contenuto prescritto dal GDPR e dovrà tener conto delle prescrizioni impartite dal Gruppo ex art. 29 (ora Comitato europeo per la protezione dei dati) nonché dal Garante per la protezione dei dati personali.
Il registro deve essere continuamente aggiornato e, se richiesto, messo a disposizione delle autorità di controllo.
Tale registro contiene le seguenti informazioni:

1. il nome e i dati di contatto del Comune di Borghetto Santo Spirito (SV), del Sindaco e/o del suo Delegato, eventualmente del Contitolare del trattamento, del Responsabile per la protezione dei dati;
2. le finalità del trattamento;
3. una descrizione sintetica delle categorie di interessati e delle categorie dei dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
5. l'eventuale trasferimento di dati personali presso un paese terzo o un'organizzazione internazionale;
6. una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali e dal Regolamento Comunale vigente in materia di trattamento dati personali;
7. il richiamo, ove possibile, alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come previste dall'art. 32, paragrafo 1 del GDPR;

8. indicazione dei termini ultimi, ove previsti, per la cancellazione delle diverse categorie di dati trattati.

Una elaborazione cartacea del registro è sottoposta all'approvazione della Giunta comunale con cadenza almeno annuale mentre una sua copia informatica è posta in conservazione sostitutiva. Tale registro non è soggetto a pubblicazione per ragioni di riservatezza.

Ciascun soggetto designato ha la responsabilità, relativamente al settore di rispettiva competenza, di effettuare periodicamente la ricognizione integrale dei trattamenti svoti, aggiornando i relativi registri di trattamento.

Spetta ai Responsabili di P.O.:

- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ufficio, al fine di consentire la compilazione del registro;
- la responsabilità relativa alla gestione del registro e del suo aggiornamento con la supervisione del DPO;
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati, da sottoporre all'approvazione del Titolare;
- la regolare tenuta del registro in relazione ai trattamenti della struttura organizzativa di competenza, fornendo le necessarie informazioni e valutazioni con la supervisione del Responsabile della gestione del registro;

Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamento è demandata alla figura del DPO.

Ai sensi dell'art. 39 del GDPR che disciplina infatti le prerogative del Responsabile della protezione dei dati personali si evince che tra le altre è tenuto a "*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*".

VALUTAZIONI DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Nel caso in cui una tipologia 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 Responsabile di P.O. competente in relazione al trattamento interessato, prima di effettuare il trattamento ed in collaborazione con il DPO, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

La valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

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 così come redatti e pubblicati dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del GDPR.

La DPIA si sostanzia in 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, valutando detti rischi e predeterminando le misure per affrontarli.

Tale procedura viene realizzata *ex ante* rispetto al trattamento dati, dal Titolare del trattamento quando una tipologia di trattamento, considerata la natura, il contesto, le finalità di detto trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, consultando preventivamente l'autorità di controllo, per il tramite dell'RPD/DPO, nel caso in cui le misure tecniche e organizzative, da loro stessi individuate per mitigare l´impatto del trattamento, non siano ritenute

sufficienti: in altri termini, qualora il rischio residuale per i diritti e le libertà degli interessati rimanga elevato.
Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo processo di DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.
La valutazione, come illustrato precedentemente, viene effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di *privacy by design* e *by default* per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi.
L'aggiornamento della valutazione d'impatto sulla protezione dei dati, nel corso dell'intero ciclo di vita del progetto, garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità.
Il Responsabile di P.O. conduce quindi una prima fase di valutazione preliminare, il cui scopo è quello di raccogliere tutte le informazioni necessarie a valutare *in primis* se il trattamento sia conforme al GDPR e, *in secundis*, comprendere se quel trattamento debba essere sottoposto ad una valutazione DPIA. L'attività quindi si scompone di 3 sotto fasi:

a) descrizione del trattamento (le categorie di soggetti interessati dal trattamento, le finalità del trattamento, le categorie di dati oggetto del trattamento, le modalità di trattamento, il luogo di conservazione dei dati trattati, …) sulla scorta delle risultanze contenute nell'apposito registro;
b) valutazione della conformità (analisi della necessità e della proporzionalità del trattamento rispetto alle finalità; rispetto dei principi applicabili al trattamento di cui al capo II del GDPR; rispetto dei diritti degli interessati di cui al capo III del GDPR);
c) valutazione della obbligatorietà di condurre una DPIA;

Fermo restando quanto indicato dall'art. 35, paragrafo 3, del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

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

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Responsabile di P.O. competente in relazione al trattamento interessato, sentito il Responsabile della protezione dei dati e l'Amministratore del sistema informatico (se esistente), ritenga motivatamente che non possa presentare un rischio elevato; il Responsabile di P.O. competente in relazione al trattamento interessato può, motivatamente, ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

La DPIA non è necessaria nei casi seguenti:

a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del GDPR;
b) 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;
c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
d) 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 inoltre necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità di controllo o dal Responsabile della protezione dei dati personali e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni dell'Autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

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

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
    1) delle finalità specifiche, esplicite e legittime;
    2) della liceità del trattamento;
    3) dei dati adeguati, pertinenti e limitati a quanto necessario;
    4) del periodo limitato di conservazione;
    5) delle informazioni fornite agli interessati;
    6) del diritto di accesso e portabilità dei dati;
    7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
    8) dei rapporti con i responsabili del trattamento;
    9) delle garanzie per i trasferimenti internazionali di dati;
    10) 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;
e) l'acquisizione del parere del Responsabile della protezione dei dati personali.
f) Assume quindi fondamentale importanza l'attività di formalizzazione dei risultati la quale consiste nel valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le

attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla consultazione preventiva.

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un documento finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR. Il documento deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

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

Il Responsabile di P.O. competente in relazione al trattamento interessato garantisce l'effettuazione della DPIA ed è responsabile della stessa, salvo che ne affidi l'esecuzione ad altro soggetto, anche esterno al Comune. Deve consultarsi con il Responsabile della protezione dei dati personali anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Responsabile di P.O. competente in relazione al trattamento interessato devono essere documentate nell'ambito della DPIA.

Il servizio interessato deve consultare l'Autorità di controllo prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato (tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il GDPR, in particolare qualora non abbia identificato o attenuato sufficientemente il rischio). Lo stesso sente e valuta insieme al Garante per la protezione dati personali anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo.

Salvo diversa disposizione dell'Autorità stessa è bene che la comunicazione di richiesta di consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data.

L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

Il processo DPIA deve sempre prevedere un monitoraggio dei risultati raggiunti ed un conseguente e costante riesame al fine di garantire nel tempo la mitigazione dei rischi e la conformità al GDPR, anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno ed esterno, finalità del trattamento, strumenti utilizzati, organizzazione comunale, presenza di nuove minacce, ecc.).

Il DPO/RPD monitora lo svolgimento della DPIA. Può inoltre proporre lo svolgimento di una valutazione 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.

Eventuali altri Responsabili del trattamento collaborano e assistono il servizio interessato oltre che il Responsabile della protezione dei dati nella conduzione della DPIA fornendo ogni informazione necessaria.

L'Amministratore del sistema informatico fornisce il necessario supporto al Responsabile di P.O. competente in relazione al trattamento interessato. Può inoltre proporre di condurre una DPIA in relazione ad uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

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.

Dal punto di vista operativo - considerata la complessità di un processo DPIA e relativa fase di analisi dei rischi – l'Ufficio deve adottare strumenti applicativi specializzati in grado di gestire tutte le fasi del processo ed in grado di riproporre la sua applicabilità nel tempo.[1.]
È pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

VIOLAZIONE DEI DATI PERSONALI

Per violazione dei dati personali (in seguito anche "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune di Borghetto Santo Spirito.
Il Titolare ha predisposto un'idonea procedura organizzativa interna corredata da apposita modulistica per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (Data breach policy).
I dati oggetto di riferimento saranno i dati personali trattati "da e "per conto" del Titolare, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.
L'obiettivo del presente documento sarà, pertanto:

- sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
- definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
- assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate.

A tale proposito si richiama integralmente la deliberazione di Giunta comunale n. 83 del 17.08.2021 avente ad oggetto " APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)" ed i rispettivi allegati, che anche se non materialmente unito al presente ne costituisce parte integrante e sostanziale.

ACCESSO CIVICO GENERALIZZATO E PROTEZIONE DATI PERSONALI

Con specifico riferimento alla normativa in materia di trasparenza, il D.L. 97/2016, di modifica del D.lgs. 33/2013 ha introdotto l'istituto dell'accesso civico "generalizzato", che attribuisce a "chiunque" il "diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione.
L'esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis" del d.lgs. n. 33/2013). L'art. 5, c. 5, d.lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.

---

[1] *Un esempio di un software applicativo per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di CNIL (Autorità francese per la protezione dei dati). Il software, al quale ha aderito anche il Garante Italiano, non costituisce un modello al quale fare sempre riferimento (si ricorda che è stato concepito soprattutto per le PMI), ma può offrire un focus sugli elementi principali di cui si compone la procedura di DPIA. Può quindi costituire un utile supporto metodologico e di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate. Può servire inoltre per comprendere meglio quali possono essere i requisiti di base di un applicativo DPIA adeguato alla propria realtà procedendo quindi ad una software selection più mirata e consapevole.*

Il Comune di Borghetto Santo Spirito ha emanato un Regolamento denominato “Regolamento comunale per l'accesso civico e l'accesso generalizzato” approvato con Deliberazione del Commissario straordinario con i poteri della Giunta Comunale n. 16 del 30.01.2017 che disciplina le modalità organizzative adottate dall’Ente per l’esercizio di tali diritti.
Si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture dell’Ente, e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.) in materia di accesso civico generalizzato e protezione dei dati personali, il RPD funge da supporto ai Servizi competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti alle richieste di accesso civico generalizzato.
Altresì, il RPD funge da supporto al RPCT nei casi di riesame di istanze di accesso negato o differito a tutela dell’interesse alla protezione dei dati personali.
Inoltre, il RPD, su richiesta dei Servizi, fornisce il proprio parere in ordine alla valutazione dell’eventuale pregiudizio che l’accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell’art. 5-bis e, in via generale, del GDPR.
Sempre il DPO, su richiesta dei Servizi, fornisce il proprio parere in ordine all’opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi relativi alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti. Alla luce di tale parere, i Servizi competenti relativamente alle singole richieste di accesso effettueranno il bilanciamento tra gli interessi lesi e la rilevanza dell’interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

PARTE IV - DIRITTI DELL'INTERESSATO

INFORMATIVA, COMUNICAZIONE E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Il Comune adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli art. 13 e 14 del GDPR nonché per gestire le comunicazioni in merito all'esercizio dei diritti riconosciuti dal 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.
Le informative sono fornite mediante predisposizione di idonea pagina web sul sito istituzionale e mediante pubblicazione del relativo testo all'Albo pretorio e nella sezione Amministrazione trasparente del portale (Informativa estesa). Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del Comune è predisposta apposita informativa.
Un'informativa breve è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati; nel modulo sono indicati i soggetti ai quali l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture comunali, nelle sale d'attesa ed in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- in 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 Comune;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutte le comunicazioni dirette all'Amministrazione;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, ecc.

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
Il Comune agevola l'esercizio dei diritti dell'interessato ai sensi degli art. da 12 a 18 del GDPR. Nei casi di cui all'art. 11, paragrafo 2, del GDPR il Comune non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli art. da 12 a 18, salvo che dimostri che di non essere in grado di identificare l'interessato.
L'Ente fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta di esercizio dei diritti riconosciuti dal GDPR, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Comune informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.
Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con gli stessi mezzi, salvo diversa indicazione dell'interessato.
Se non ottempera alla richiesta dell'interessato, il Comune informa lo stesso senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
Le informazioni fornite ed eventuali comunicazioni e azioni intraprese sulla base dei diritti riconosciuti dal GDPR sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Comune può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta;

oppure

b) rifiutare di soddisfare la richiesta. Incombe al Comune l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Fatto salvo l'articolo 11 del GDPR, qualora il Comune nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di esercizio dei diritti riconosciuti dal GDPR, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

ELENCO ALLEGATI

1 - Finalità di trattamento;
2 - Organigramma Privacy Ente;

3 - Modello generico di informativa;

4 - Schema elenco Responsabili trattamento dati personali dell'Ente;

5 - Modello generico atto di designazione / autorizzazione;

6 - Appendice normativa.

Costituisce altresì allegato integrale e sostanziale, anche se non materialmente unito al presente, la DGC n. 83 del 17.08.2021 avente ad oggetto "APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)".
