# COMUNE DI BORGONE SUSA

CITTA' METROPOLITANA DI TORINO

# REGOLAMENTO PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

**Approvato con deliberazione del _____n. _____del _____**

**INDICE**

**Art. 1 (Oggetto)**

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Borgone Susa.

**Art. 2 (Titolare del trattamento)**

1. Il Comune di Borgone Susa, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato le informazioni indicate nel GDPR.

5. Il Titolare del trattamento provvederà a effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") nei casi previsti dall'art. 35 del RGDP.

6. Il Titolare, inoltre, osserverà le disposizioni seguenti.
a) In base all'articolazione interna dell'Ente i responsabili degli uffici o dei servizi in cui si articola l'organizzazione comunale, cureranno sotto la propria responsabilità che siano rispettati gli adempimenti previsti dal regolamento UE 2016/679 nei trattamenti di tutti i dati personali effettuati nelle articolazioni organizzative di loro competenza;
b) Il Comune nomina il Responsabile della protezione dei dati;
c) Il Comune nomina quale Responsabile del trattamento (e disciplina il relativo rapporto ai sensi dell'art. 28 del regolamento UE 2016/679) i soggetti pubblici o privati che per qualunque ragione o titolo trattano per conto del Comune dati personali di cui il Comune è titolare del trattamento;

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da altri enti ed organismi, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità

di cui all'art. 26 del RGPD.

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

**Art. 3 (Finalità del trattamento)**

1. I trattamenti sono compiuti dal Comune per le finalità e nell'ambito di cui all'articolo 6 del Regolamento UE 2016/679.

**Art. 4 (Esecuzione degli adempimenti previsti dal regolamento UE 2016/679)**

1. I responsabili degli uffici o dei servizi in cui si articola l'organizzazione comunale, che ai sensi dell'articolo 2 comma 6) lettera a) del presente Regolamento cureranno sotto la propria responsabilità che siano rispettati gli adempimenti previsti dal regolamento UE 2016/679 in tutti i trattamenti dei dati personali effettuati dalle articolazioni organizzative di loro competenza, provvederanno tra l'altro:
- alla tenuta del registro delle categorie di attività di trattamento svolte sotto la propria responsabilità;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- agli adempimenti previsti dal Regolamento 2016/679 per i casi di violazione dei dati personali (cd. "*data breach*").

**Art. 5 (Responsabile della protezione dati)**

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato in una figura unica, dipendente di ruolo del Comune, o un professionista esterno.
Il RPD può essere scelto fra i dipendenti del Comune, purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
Nel caso in cui il RPD non sia un dipendente dell'Ente, l'incaricato persona fisica è selezionato fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al RPD sono indicati in apposito contratto di servizi. Il RPD esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento.
Il RPD è incaricato dei compiti indicati all'articolo 39 del GDPR.

2. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

3. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle capacità di bilancio dell'Ente.

5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il Titolare del trattamento fornisce al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
Il RPD non può essere rimosso o penalizzato dal Titolare e dai Responsabili del trattamento per l'adempimento dei propri compiti.
Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

**Art. 6 (Sicurezza del trattamento)**

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

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento sono determinate ai sensi dell'articolo 32 GDPR.

3. Costituiscono, a mero titolo di esempio, misure tecniche ed organizzative che possono essere adottate dai responsabili degli uffici o dei servizi in cui si articola l'organizzazione comunale:
- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

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

5. Il Comune di Borgone Susa si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I dati di contatto del Titolare e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

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

**Art. 7 (Registro delle attività di trattamento)**

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le indicazioni di cui all'art. 30 GDPR e il relativo modello sarà approvato dalla Giunta comunale.

**Art. 8 (Registro delle categorie di attività trattate)**

1. Nel caso in cui il Comune di Borgone Susa operi come Responsabile del trattamento per conto di altri Enti sarà tenuto ad adottare e aggiornare il Registro delle categorie di attività trattate ai sensi dell'art. 30 comma 2 GDPR e il relativo modello sarà approvato dalla Giunta comunale.

**Art. 9 (Valutazioni d'impatto sulla protezione dei dati)**

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, 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 DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35, pp. 4-6, del RGDP.

**Art. 10 (Violazione dei dati personali)**

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

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

2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

**Art. 11 (Rinvio)**

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