



COMUNE DI RIVA DEL PO

Provincia di Ferrara

Via 2 febbraio, 23 - 44033 - Riva del Po - loc. Berra

Sede distaccata: Piazza Libertà 1 - 44030 - Riva del Po - loc. Ro



➤ [Approvate con Delibera di Giunta Comunale n. 48 del 07-07-2022](#)

MISURE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. Finalità

Obiettivo del presente documento è di definire il Modello Organizzativo in materia di trattamento dei dati personali al fine di implementare una strategia per il trattamento dei dati personali effettuato dall'ente, ai sensi del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (Codice della Privacy), come modificato dal D.Lgs. 10 agosto 2018, n. 101 e del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (GDPR - General Data Protection Regulation). Con il presente atto sono quindi definiti i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice della Privacy" e del "GDPR".

Il Comune, nell'assolvimento delle proprie finalità istituzionali, secondo i principi di trasparenza, efficacia ed economicità, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto alla riservatezza ed all'identità personale nonché delle norme vigenti in materia di protezione e gestione dei dati.

In adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa, favorisce la trasmissione di dati e documenti tra le banche dati e gli archivi del Comune, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea.

La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità;

Ai fini del presente atto, per finalità istituzionali del Comune si intendono le funzioni ad esso attribuite dalle leggi, dallo Statuto e dai regolamenti o per effetto di accordi e/o convenzioni.

I trattamenti sono compiuti dal Comune per le seguenti finalità:

- a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:
 - o l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
 - o la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
 - o l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.
- b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
- c) l'esecuzione di un contratto con soggetti interessati;
- d) le specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

L'ente si impegna a garantire che il trattamento dei dati personali avvenga in maniera conforme a quanto previsto dalla normativa e, secondo i seguenti principi di liceità, questi sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito si impegna ad adottare misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservare i dati 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;
- trattare i dati 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.

CAP. I – MISURE ORGANIZZATIVE

2. Il titolare

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è **l'Ente Comune di Riva del Po** cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Spetta pertanto in particolare all'Ente:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali oggetto di prossimo adeguamento al Regolamento;
- designare il Responsabile della protezione dei dati;
- designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
- effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
- istruire i soggetti autorizzati al trattamento dei dati personali.

3. I Designati

Sono individuati quali **designati**, ai sensi dell'art. 2-quaterdecies del D.lgs. 196/2003 e ss.mm.ii., **i Responsabili di Settore del Comune di Riva del Po**, ciascuno per il proprio ambito di attività, i quali operano con il supporto giuridico del Segretario Comunale.

Relativamente ai trattamenti di dati personali trasversali a più settori si applica il criterio della prevalenza.

Di seguito, sono indicati i compiti affidati ai soggetti designati quali responsabili Interni del Trattamento dei Dati:

- 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. tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
- E. predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;
- F. individuare i soggetti autorizzati a compiere operazioni di trattamento, fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;

- G. predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
- H. provvedere, anche tramite gli i soggetti autorizzati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
- I. disporre l'adozione dei provvedimenti imposti dal Garante;
- J. collaborare attivamente con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
- K. adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri con altri Soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;
- L. 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;
- M. garantire al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
- N. effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, 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;
- O. 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'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
- P. individuare e nominare i Responsabili esterni di trattamento e conservare il relativo Registro delle attività di trattamento;
- Q. rilevare e comunicare i casi di violazione dei dati personali, nell'ambito organizzativo di riferimento (data breach).

4. Responsabilità per le procedure di trattamento dati

Ai Responsabili di Area del Comune di Riva del Po è attribuita la responsabilità per il trattamento dei dati afferenti il Settore di competenza.

Sono designati, inoltre, Responsabili del trattamento di dati personali, i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare.

Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali dell'affidatario dell'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale.

5. Autorizzati al Trattamento

Sono autorizzati al compimento alle operazioni di trattamento dei dati, i Designati di cui al precedente paragrafo ed i funzionari da loro delegati quali referenti autorizzati, ai sensi della presente disciplina, che conformano i loro trattamenti alle policy dell'Ente in materia di protezione dei dati personali e alle istruzioni di seguito riportate:

- sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- sono verificati legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Sono, altresì, autorizzati tutti i soggetti che effettuino operazioni di trattamento, dipendenti e collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare o dei soggetti delegati quali referenti autorizzati. Tali soggetti devono essere da questi formalmente autorizzati.

Gli autorizzati al trattamento sono quindi individuati:

- tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;
- tramite assegnazione funzionale della persona fisica alla unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

La designazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento.

Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alle policy dell'Ente in materia di sicurezza informatica e protezione dei dati personali.

6. Il Responsabile della Protezione dei dati (DPO)

Il "Regolamento (UE) 2016/679" del Parlamento Europeo e del Consiglio del 27 aprile 2016 prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO).

Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli art. 37 e ss del suddetto regolamento, conformati alla precipua organizzazione dell'Ente:

- informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto del Segretario Comunale e dei Responsabili di Settore ;
- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente 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;
- coopera con il Garante per la protezione dei dati personali;
- funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
- partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;
- formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento.
- fornisce i pareri obbligatori e facoltativi richiesti dall'Ente;

7. Accesso civico generalizzato e ruolo DPO

Con specifico riferimento alla normativa in materia di trasparenza, 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.).

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.

Il DPO funge da supporto alle strutture 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 le richieste di accesso civico generalizzato.

Il DPO funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.

Il DPO, inoltre, su richiesta delle strutture, esprime 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 Regolamento UE n. 679/2016.

Il DPO, su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'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 opposenti.

Sulla scorta di tale parere le strutture competenti sulle singole richieste di accesso effettueranno il bilanciamento tra l'interesse alla protezione dei dati personali e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare, che deve essere finalizzato essenzialmente al controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.

CAP. I – MISURE GENERALI

8. Trattamenti consentiti.

Il Comune, di norma, non è tenuto a chiedere il consenso al trattamento dei dati da parte degli interessati.

La pubblicazione e la divulgazione di atti e documenti che determinano una "diffusione" dei dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di cittadini, è legittima solo se la diffusione è prevista da una norma di legge o di regolamento.

Prima della pubblicazione di dati personali deve essere valutato se le finalità di trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.

Se risulta possibile occorre citare i dati personali solo negli atti a disposizione degli uffici, richiamati quale presupposto della deliberazione e consultabili solo da interessati e controinteressati oppure utilizzare espressioni di carattere generale, soprattutto nel quadro dell'attività di assistenza e beneficenza, che spesso comporta la valutazione di circostanze e requisiti personali che attengono a situazioni di particolare disagio.

Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.

Per attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione, anche successivo, del consenso al trattamento.

Negli atti destinati alla pubblicazione o divulgazione i dati che permettono di identificare gli interessati sono riportati solo quando è necessario ed è previsto da una norma di legge, rispettando il principio di proporzionalità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.

I sistemi informativi ed i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estratti degli atti con l'esclusione dei dati personali in essi contenuti.

9. Attività amministrativa

L'attività amministrativa del Comune si svolge, principalmente, con l'emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.

Per l'attività informatica di cui al comma precedente sono rigorosamente rispettate le norme di cui al codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni.

La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

10. Sicurezza dei dati – Misure di sicurezza – Verifiche e controlli

1. Tutta l'attività di gestione è finalizzata a:

- a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati;
- b) evitare l'accesso, non autorizzato, alle banche dati, alla rete e, in generale, ai servizi informatici del Comune;
- c) prevenire:
 - trattamenti dei dati non conformi alla legge o ai regolamenti;
 - la cessione o la distribuzione dei dati in caso di cessazione del trattamento.

I responsabili esterni del trattamento (opportunamente nominati) garantiscono, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, l'adozione e lo sviluppo di misure di sicurezza adeguate come: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nella gestione dei dati personali con il sistema informatizzato dovrà essere assicurato il puntuale e scrupoloso rispetto di tutte le norme vigenti.

Gli stessi responsabili delle banche dati si attiveranno periodicamente con controlli, anche a campione, al fine di garantire la sicurezza delle banche dati e la esattezza e completezza dei dati inseriti.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal servizio cui è preposto ciascun autorizzato al trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

Ogni ulteriore misura idonea a tutela delle banche dati personali informatiche o cartacee andrà adottata secondo un principio di proporzionalità tra le risorse disponibili e i diritti da tutelare.

11. Indicazioni operative per gli autorizzati al trattamento dei dati

Di seguito sono elencati i comportamenti virtuosi da applicare:

- la pubblicazione dei dati personali contenuti in atti e/o documenti dovrà avvenire nel pieno rispetto delle Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati (pubblicato sulla gazzetta ufficiale n. 134 del 12 giugno 2014);
- i dipendenti autorizzati sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;

- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi/dispositivi utilizzati per accedere alle informazioni riservate e/o ai dati sensibili e/o alle categorie particolari di dati personali non devono essere lasciate su una scrivania non presidiata;
- le password non possono essere lasciate su note adesive attaccate sopra, sotto o nei pressi di un computer, né possono essere lasciate per iscritto in posizione accessibile;
- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere distrutti e, ove presenti, triturati nei distruggidocumenti appositi;
- le lavagne/appunti contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere cancellate;
- i dispositivi portatili come smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere conservati in cassette chiuse a chiave.

La violazione delle sopra elencate indicazioni operative è fonte di responsabilità disciplinare ai sensi del CCNL di categoria e dalla normativa in vigore.