



COMUNE DI OFFIDA

Regolamento per la protezione dei dati personali

in attuazione del Regolamento UE 2016/679

Art. 1 – Oggetto
Art. 2 – Finalità del trattamento
Art. 3 – Titolare del trattamento
Art. 4 – Contitolari del trattamento
Art. 5 – Responsabile del trattamento
Art. 6 – Responsabile della protezione dei dati
Art. 6 – Trattamento di dati personali nei servizi esternalizzati
Art. 8 – Sicurezza del trattamento
Art. 9 – Registro unico delle attività di trattamento
Art. 10 – Violazione dei dati personali
Art. 11 – Affidamento a soggetti esterni
Art. 12 – Pubblicazione

Allegati:

- A) Modello gestione privacy
- B) Modello Registro

Articolo 1

Oggetto

Il presente Regolamento disciplina le misure procedurali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo n. 679 del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" (RGPD), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nonché alla libera circolazione di tali dati, per il Comune di Offida.

Articolo 2

Titolare del trattamento

1. Il Comune di Offida è il titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee, gestite dagli uffici comunali.
2. Le funzioni attribuite al Comune in qualità di Titolare del trattamento sono esercitate dal Sindaco che le può delegare, anche parzialmente, a un Assessore o al Segretario comunale.
3. Il Comune 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.
4. Il Comune 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.
5. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
6. Il Titolare adotta misure appropriate per fornire all'interessato:
 - a) le informazioni indicate dall'art. 13 del RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
 - b) le informazioni indicate dall'art. 14 del RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.
7. 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 Comune deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con DPIA) ai sensi dell' art. 35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 36.
8. Il Sindaco provvede a:
 - a) nominare il Responsabile della protezione dei dati;
 - b) designare il Responsabile del trattamento;
 - c) diramare le direttive necessarie per l'applicazione delle disposizioni del RGPD e del presente Regolamento, sentito il Segretario comunale
9. Nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o in altri strumenti giuridici consentiti dalla legge con cui è affidata a soggetti esterni al Comune la gestione di attività e/o servizi per conto dell'Amministrazione comunale, è prevista espressamente la nomina degli stessi soggetti affidatari quali responsabili del trattamento dei dati personali connessi alle attività istituzionali affidate.

Articolo 3

Finalità del trattamento

1. I trattamenti dei dati personali sono compiuti per le seguenti finalità:
 - a. l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
Rientrano in questo ambito i trattamenti compiuti per:
 - l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed

utilizzazione del territorio e dello sviluppo economico;

- la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
 - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.
 - l'esercizio dell'attività contrattuale con soggetti interessati.
 - l'esercizio di altri compiti istituzionali legati al Comune.
- b. specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Articolo 4 Contitolari del trattamento

1. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali, regionali o locali, allorché due o più titolari determinano congiuntamente e in modo trasparente, mediante accordo interno, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del RGPD.

2. L'accordo definisce le responsabilità di ciascun titolare in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa europea o statale specificatamente applicabile. Tale accordo può individuare un punto di contatto comune per gli interessati.

Articolo 5 Responsabile del trattamento

1. Il Comune si avvale del Responsabile del trattamento, designato dal Sindaco. La designazione avviene con l'atto di attribuzione delle funzioni, nel quale sono previsti:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati,
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Responsabile del trattamento.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Comune e ciascun responsabile designato qualora si tratti di soggetto esterno.

2. Può essere designato Responsabile del trattamento dei dati personali, contenuti in tutte le banche dati esistenti nell'articolazione organizzativa di rispettiva competenza, il Segretario o un dipendente cui è attribuita la Posizione Organizzativa o un dipendente responsabile di un servizio o di un ufficio che abbia una rilevante importanza per l'attività istituzionale dell'Ente.

3. Il Responsabile del trattamento deve essere messo in grado, anche attraverso una adeguata preventiva formazione, di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità e di adottare le misure tecniche e organizzative di cui all'art. 28 del RGPD, rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

4. Qualora il Responsabile del trattamento si assenti o sia impedito o sospeso per un prolungato periodo di tempo superiore a trenta giorni, il Sindaco può procedere alla nomina di supplenti che abbiano i requisiti richiesti.

5. Il Responsabile del trattamento provvede a:

- a) elaborare e tenere aggiornato il registro delle attività di trattamento;
- b) adottare le misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
- c) autorizzare i dipendenti interessati ad accedere ai dati personali al fine di svolgere il trattamento afferente ai rispettivi compiti istituzionali;
- d) fornire le istruzioni per il corretto trattamento dei dati personali, e controllare che le attività di trattamento, con particolare riferimento alle operazioni di comunicazione e diffusione, svolte dagli incaricati siano conformi alle norme del RGPD;
- e) segnalare al Titolare l'eventuale esigenza di definire la valutazione dell'impatto sulla protezione dei dati

- (DPIA) fornendo allo stesso ogni informazione di cui è in possesso;
- f) informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante per la protezione dei dati personali, nel caso in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.
- g) assicurare il rispetto delle regole previste nel modello di gestione privacy del Comune secondo lo schema di cui all'allegato A al presente regolamento.
- h) adottare le misure necessarie per facilitare l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGDP;
- i) svolgere tutti gli altri compiti indicati nell'atto di designazione.
6. Il Responsabile del trattamento provvede, nell'ambito dei propri poteri di controllo, a effettuare periodiche verifiche sulla corretta applicazione della normativa in materia di trattamento dei dati personali, in accordo con i controlli specifici effettuati dal Responsabile della protezione dei dati.

Articolo 6

Responsabile della protezione dei dati

1. Il Comune si avvale di un Responsabile della protezione dei dati (RPD), in possesso di adeguate qualità professionali, e della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.
2. Il Responsabile della protezione dei dati è designato con atto del Sindaco.
3. Può essere designato RDP il Segretario o un Dirigente o un dipendente a tempo indeterminato di questo Comune inquadrato in una categoria non inferiore alla C) o anche un soggetto esterno, persona fisica che sia in possesso delle qualità di cui al comma 1. La designazione da parte del Sindaco del soggetto esterno avviene tra quanti abbiano partecipato ad una apposita procedura ad evidenza pubblica e assolve i suoi compiti in base a un contratto di servizio sottoscritto dal Dirigente del settore Affari Generali. L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del RPD. Va in ogni caso assicurata l'assenza di conflitto di interessi con le mansioni esercitate e attribuite.
4. I dati identificativi e di contatto del Responsabile della protezione dei dati sono:
 - pubblicati nel sito web istituzionale dell'Ente, rendendoli accessibili;
 - comunicati al Garante per la protezione dei dati personali;
 - comunicati ai componenti degli organi di governo, a tutti i dipendenti comunali, ai componenti degli organi di controllo interni.
5. Sino alla designazione del nuovo RPD si intende prorogata di diritto la designazione del Responsabile della protezione dei dati in carica.
6. Il Responsabile della protezione dei dati provvede a:
 - a) informare e fornire consulenza al Titolare del trattamento e al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento e dalle disposizioni dell'UE e nazionali relative alla protezione dei dati;
 - b) sorvegliare l'osservanza del RGPD e di altre disposizioni vigenti in materia di protezione dei dati da parte del Titolare del trattamento e del Responsabile del trattamento;
 - c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo attuate dal Titolare e dal Responsabile del trattamento;
 - d) fornire, se richiesto dal Titolare, il parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
 - e) vigilare sullo stato di attuazione del sistema di protezione dei dati personali.
 - f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto con detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del RGPD, ed effettuare eventuali consultazioni.
 - g) verificare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

7. Il Titolare del trattamento e il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente informato in tutte le questioni riguardanti la protezione dei dati personali.
8. Il RPD è tenuto a segnalare al Sindaco, al Segretario comunale e al Responsabile del trattamento eventuali decisioni o provvedimenti o comportamenti adottati che risultino incompatibili con il RGPD.
9. Il Titolare del trattamento fornisce al Responsabile della protezione dei dati, nell'esecuzione dei compiti di cui all'articolo 39 del RGPD, le risorse necessarie per assolvere tali compiti.
10. Gli interessati possono contattare direttamente il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento
11. Il Responsabile della protezione dei dati è tenuto alla riservatezza in merito all'adempimento dei propri compiti, in conformità della normativa UE e nazionale.

Articolo 7

Trattamento di dati personali nei servizi esternalizzati

1. Nell'ipotesi in cui a soggetti pubblici o privati esterni sia affidata, tramite delega o concessione o contratto, lo svolgimento di compiti e/o servizi di competenza del Comune che implicano il trattamento di dati personali, l'atto di affidamento deve prevedere norme specifiche rivolte ad assicurare l'osservanza del RGPD e ad indicare il responsabile esterno del trattamento. In particolare l'atto deve prevedere la nomina del legale rappresentante del soggetto pubblico o privato ovvero la persona fisica affidatario quale responsabile esterno del trattamento dei dati personali per la durata dell'affidamento e l'obbligo del soggetto affidatario ad osservare le prescrizioni di cui al RGPD , della normativa nazionale in materia di protezione dei dati personali e delle disposizioni del presente Regolamento in quanto applicabili.
2. Nelle ipotesi di trattamento dei dati personali di cui al precedente comma, il Responsabile del trattamento interessato, verifica che il soggetto esterno osservi le predette prescrizioni.

Articolo 8

Misure per la sicurezza dei dati personali

1. Le misure tecniche e organizzative di sicurezza da mettere in atto per garantire un livello di sicurezza adeguato al rischio sono:
 - tecniche di conservazione dati (pseudonimizzazione, cifratura)
 - l'uso di strumenti idonei rivolti ad assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
 - procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
 - sistemi di autenticazione, autorizzazione e protezione (antivirus, firewall, antintrusione)
 - sistemi di registrazione degli accessi
 - misure di sicurezza fisiche (misure antincendio, sistemi di rilevazione di intrusione, sistemi di sorveglianza, porte, armadi e contenitori dotati di serrature)
2. La conformità del trattamento in materia di sicurezza dei dati personali prevista dal RDGP è dimostrata attraverso l'adozione di misure adeguate o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
3. Il Titolare e il Responsabile del trattamento nonché il Responsabile della protezione dei dati assicurano l'osservanza delle misure di sicurezza anche impartendo adeguate istruzioni.

Articolo 9

Registro unico delle attività di trattamento

1. E' istituito il Registro unico delle attività di trattamento, tenuto dal Responsabile del trattamento, nel quale sono annotate le seguenti informazioni:
 - a) il nome ed i dati di contatto del Titolare del trattamento, del Responsabile del trattamento e del Responsabile della protezione dei dati;
 - b) le categorie di trattamenti effettuati: raccolta, registrazione, conservazione, estrazione, consultazione,

- uso, comunicazione, divulgazione, raffronto, limitazione, cancellazione, distruzione;
- c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- f) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
- g) ogni altra informazione necessaria
2. E' facoltà del Titolare del trattamento, sentiti il Responsabile del trattamento e il Responsabile della protezione dei dati, estrapolare i dati attinenti ai rischi rilevati, alla loro ponderazione e alle rispettive misure individuate, annotandoli in un distinto apposito registro denominato Registro dei rischi e delle misure.
3. Il Registro unico delle attività di trattamento, tenuto in formato informatico, è compilato sotto la responsabilità del Responsabile del trattamento, conformemente allo schema di cui all'allegato B al presente regolamento.
4. Il Registro è aggiornato almeno ogni sei mesi.

Articolo 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 dal Comune.
2. 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:
- a) danni fisici, materiali o immateriali alle persone fisiche;
- b) perdita del controllo dei dati personali;
- c) limitazione dei diritti, discriminazione;
- d) furto o usurpazione d'identità;
- e) perdite finanziarie, danno economico o sociale.
- f) decifratura non autorizzata della pseudonimizzazione;
- g) pregiudizio alla reputazione;
- h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
3. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, informa questi ultimi, senza ingiustificato ritardo, comunicando loro la natura della violazione dei dati personali verificatesi.
- I rischi per i diritti e le libertà degli interessati si considerano elevati quando la violazione:
- coinvolge un rilevante quantitativo di dati personali e/o di soggetti interessati;
 - riguarda categorie particolari di dati personali;
 - comprende dati che possono accrescere ulteriormente i potenziali rischi (dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
 - comporta rischi imminenti e con un'elevata probabilità di accadimento (rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito, ecc.);
 - impatta su soggetti che possono essere considerati vulnerabili per le loro condizioni (utenti deboli, minori, soggetti indagati).
4. La notifica al Garante delle violazioni dei dati è effettuata dal Titolare del trattamento con le modalità previste dall'art. 33 del RGPD. La comunicazione all'interessato deve contenere le informazioni e le misure di cui all'art. 34 del RGPD.
5. Il Titolare del trattamento deve documentare le violazioni di dati personali rilevate, 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 agli atti in quanto può essere richiesta dal Garante per la protezione dei dati personali al fine di verificare il rispetto delle disposizioni del RGPD.

Articolo 11

Affidamento a soggetti esterni

1. Per il trattamento dei dati personali nel rispetto della disciplina prevista dal RGDP e da altre fonti nazionali, il Comune può avvalersi anche di soggetti pubblici o privati esterni tramite un contratto di servizio nel quale sono specificati le finalità e le modalità del trattamento, le categorie di dati da trattare, le responsabilità e gli obblighi facenti carico al soggetto.
2. I soggetti di cui al comma 1 devono fornire le garanzie previste dall'art.5, comma 3 del presente Regolamento
3. Nell'atto di affidamento si rinvia all'osservanza delle altre disposizioni del presente Regolamento in quanto applicabili.

Articolo 12

Pubblicazione

1. Il presente regolamento, divenuto esecutivo, è pubblicato nel sito web istituzionale del Comune, nella sottosezione di secondo livello "Atti generali" della sottosezione di primo livello "Disposizioni generali" all'interno della sezione "Amministrazione trasparente".

Allegato A

Modello gestione privacy

L'allegato contiene l'insieme degli strumenti operativi da mettere in atto per assicurare l'adeguatezza del sistema di gestione privacy comunale al Regolamento Europeo sulla protezione dei dati personali.

Individuazione dei ruoli e delle responsabilità

Occorre attribuire alle persone autorizzate al trattamento ruoli e responsabilità all'interno dell'organizzazione per un corretto trattamento dei dati personali. Inoltre è importante, sulla base della nuova normativa, individuare e contrattualizzare tutti i responsabili esterni di trattamento, quali consulenti esterni e società di servizi.

Istruzioni operative

Lo scopo delle istruzioni operative è dare delle linee guida per garantire il rispetto della normativa UE 2016/679 per il trattamento e protezione dei dati personali, in particolare descrivono le procedure e le modalità operative per la corretta gestione degli strumenti informatici e cartacei.

Informative

Nel caso di trattamento dei dati in cui viene richiesto il consenso, il titolare del trattamento ha l'obbligo di fornire all'interessato tutte le informazioni relative al trattamento dei suoi dati personali e/o sensibili in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Privacy policy del sito

La privacy policy del sito descrive nella maniera più dettagliata e chiara possibile le modalità di gestione e trattamento dei dati personali degli utenti e dei visitatori del sito internet.

Gestione data breach

La gestione del data breach richiede delle regole e delle procedure per la rilevazione della violazione e la successiva notifica.

Allegato B Modello registro unico dei trattamenti

Il Garante raccomanda nelle sue Linee Guida al Regolamento di redigere il Registro dei trattamenti:

“la tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro”.

La redazione del registro è ispirata anche alle seguenti finalità:

- rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna;
- costituire lo strumento di pianificazione e controllo della politica della sicurezza di dati e banche di

dati, tesa a garantire la loro integrità, riservatezza e disponibilità.

Dal considerando 82 del Regolamento.

“Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti”.

Il modello del **Registro unico dei trattamenti** è il seguente: tabella con

righe corrispondenti ai trattamenti e colonne con:

- TRATTAMENTO
(ufficio, descrizione, tipologia, finalità, modalità)
- DATI PERSONALI
(categoria, se sensibili, conservazione)
- INTERESSATI
(categoria, fondamento del trattamento, consenso)
- DESTINATARI
(categoria, trasferimento)
- ANALISI DI RISCHIO
(rischi specifici, livello)
- MISURE DI PREVENZIONE
(organizzative, fisiche e tecniche)