All. A)

REGOLAMENTO COMUNALE

di attuazione del Regolamento UE 2016/679 (protezione delle persone fisiche con riguardo al trattamento dei dati personali).

Approvato con delibera C.C. n.... del .....

INDICE

Art.1 – Oggetto del Regolamento e principi organizzativi per la gestione dei dati.

1. Per l'Unione di Comuni della Romagna forlivese (da adesso Unione) e per i Comuni ad essa aderenti, il presente Regolamento disciplina gli **aspetti organizzativi relativi all'attuazione della normativa sul trattamento dei dati personali,** le cui fonti di regolazione restano:

   a) il Regolamento UE 2016/679 *"Regolamento generale per la protezione dei dati personali" (da adesso GDPR);*

   b) il D.lgs n. 196/2003 (Codice Privacy), come modificato dal D.lgs 101/2018, per le parti non incompatibili con il GDPR e dalla Legge 3 dicembre 2021, n. 205 di conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, (il c.d. "Decreto capienze");

   c) le linee guida ed i provvedimenti emanate dall'*Autorità nazionale privacy*.

2. Per l'attuazione del GDPR, l'Unione e i Comuni, in qualità di titolari del trattamento dei dati, programmano e mettono in atto - a livello unitario – misure tecniche ed organizzative adeguate alla tipologia dei trattamenti ed ai rischi che gli stessi possono comportare per le libertà e i diritti delle persone, perseguendo soluzioni e modalità efficaci e semplificate.
3. Il presente Regolamento costituisce parte del "Regolamento sull'ordinamento degli uffici e dei servizi", approvato con deliberazione della Giunta comunale n. 85/2010 e ss.mm. e ii. .
4. Ulteriori disposizioni organizzative in materia di gestione/protezione dei dati personali possono essere assunte dai segretari generali, dalla conferenza dei dirigenti, dai dirigenti e dai responsabili di servizio, secondo i rispettivi ruoli e compiti nell'ambito della struttura organizzativa degli Enti.
5. Gli obiettivi strategici e gestionali connessi con l'attuazione del GDPR dovranno essere inseriti nella programmazione di Dup e di PEG degli Enti, anche al fine della valutazione della performance di tutto il personale coinvolto.

Art. 2 – Adeguamento dei sistemi per il trattamento dei dati

1. Ai sensi dell'*art.25 del GDPR*, il trattamento e la protezione dei dati personali devono essere effettuati dagli Enti titolari, a regime, tenendo conto del contesto e della gravità dei rischi, a seconda dei diversi trattamenti:

   - nella fase di progettazione di ogni nuova tipologia di trattamento **(*"privacy by design"*)**;

- per impostazione predefinita, al fine di trattare solo i dati personali necessari per ogni specifica finalità del trattamento, attuando il "principio di minimizzazione" **("*privacy by default*")**.

Art.3 – Ruoli e responsabilità di Unione e Comuni nel trattamento dei dati

1. Ai sensi degli *artt. 4/7, 24 e 26 del GDPR* e per effetto del conferimento di tutte le funzioni dai Comuni all'Unione, l'Unione ed i Comuni aderenti sono "contitolari" del trattamento di tutti i dati personali che si riferiscono ai servizi propri dell'Unione ed ai servizi conferiti dai Comuni all'Unione; fra questi ultimi sono compresi altresì i servizi per i quali i Comuni mantengono alcune competenze proprie.
2. I predetti Enti, in qualità di "contitolari" del trattamento dei dati, esercitano poteri decisionali sulle finalità e sui mezzi del trattamento dei dati personali - a livello unitario di Unione, con modalità uniformi - secondo quanto disposto dagli Statuti degli Enti, dalle vigenti convenzioni e dal presente Regolamento organizzativo. Le decisioni strategiche vengono assunte dalla Giunta dell'Unione, mentre l'attuazione concreta delle misure tecniche e organizzative è demandata ai dirigenti e agli altri responsabili gestionali.

Art. 4 - Altri contitolari del trattamento dei dati

1. Ai sensi dell'art. 26 del GDPR, qualora siano individuabili altri soggetti "contitolari" del trattamento dei dati personali, insieme all'Unione ed ai Comuni, i rispettivi ruoli ed obblighi per gli aspetti concernenti il trattamento dei dati dovranno essere regolati all'interno di un apposito accordo/protocollo/contratto.
2. Presupposto per la contitolarità dei dati è la condivisione tra diversi titolari delle finalità e dei mezzi del trattamento dei dati personali.

Art. 5 – Ruoli e responsabilità gestionali interne per il trattamento dei dati personali

1. Per Comuni e Unione, nell'ambito della struttura organizzativa unica dell'Unione, **i dirigenti ed i responsabili dei servizi** - quali assegnatari di risorse umane, strumentali e finanziarie, nonché soggetti dotati di competenze e responsabilità gestionali, secondo le norme organizzative interne – mettono in atto misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al GDPR.

2. Essi, in particolare – con le risorse assegnate, con il supporto del gruppo di lavoro di cui all'art. 7, nonché con la consulenza del DPO di cui all'art. 11 - assicurano:

a) **la tenuta ed aggiornamento del "registro dei trattamenti"**, relativamente ai trattamenti dei dati afferenti ai servizi assegnati, come stabilito all'art. 30 del GDPR e disciplinato nel presente regolamento al successivo art. 12;

b) **i rapporti con i "responsabili dei trattamenti"**, come stabilito all'art. 28 del GDPR e disciplinato nel presente regolamento al successivo art. 6;

c) **il rispetto dei principi previsti dagli *artt. 5-11 del GDPR* da parte dei dipendenti assegnati** alle loro unità organizzative, qualora gli stessi siano designati, anche informalmente, a svolgere attività di trattamento dei dati personali, dovendo fornire agli stessi adeguate istruzioni e disposizioni organizzative/procedurali per il trattamento dei dati.

d) **il rispetto delle regole di informazione e dei diritti di trasparenza e accesso nei confronti degli interessati**, conformemente a quanto stabilito dall'art. 12 del GDPR, fornendo le "informative" di cui agli artt. 13-14 del GDPR, nonché le "comunicazioni" di cui agli artt.15/22 del GDPR, finalizzate all'esercizio dei diritti dell'interessato, per quanto applicabili e secondo le indicazioni contenute nel "registro dei trattamenti";

e) **l'adozione delle misure di sicurezza indicate all'art. 32 del GDPR** – in ambito informatico e non - adeguate alla probabilità e gravità dei rischi (distruzione, perdita, modifica, divulgazione e/o accessi non autorizzati) che riguardano gli specifici trattamenti attribuiti alla propria competenza (vedasi successivo art.10).

f) **la segnalazione delle violazioni dei dati** di cui vengono a conoscenza, come stabilito all'art. 34 del GDPR e disciplinato nel presente regolamento al successivo art. 14;

g) **il rispetto del principio di accountability/responsabilizzazione**, comprovando l'adozione delle misure organizzative/tecniche mediante l'aggiornamento del "registro degli eventi per l'accountability" di cui al successivo art. 9.

3. **I dirigenti sono chiamati a fornire supporto e risorse per le attività del GdL-privacy e del DPO,** in particolar modo qualora gli stessi non siano dotati di risorse umane, finanziarie e strumentali specificatamente assegnate dalla Giunta dell'Unione.

Art.6 – Responsabili esterni del trattamento dei dati, ai sensi dell'art. 28 GDPR

1. Secondo la definizione dell'*art.4/8 del GDPR*, *il 'responsabile del trattamento' è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*.
2. I "responsabili del trattamento" sono, di norma, **soggetti/enti/società esterni che trattano i dati personali per conto dell'Unione e dei Comuni,** titolari dei dati. Gli stessi devono fornire agli Enti garanzie sufficienti e mettere in atto misure tecniche ed organizzative adeguate alle modalità di trattamento dati previste dal GDPR.

3. I "responsabili del trattamento" – che hanno rapporti con l'Unione e con i Comuni effettuando per conto degli stessi il trattamento di dati personali – sono censiti nell'ambito dei diversi settori/servizi dell'Unione e dei Comuni, al fine di essere formalmente designati ai sensi dell'art. 28 del GDPR, con gli atti di cui ai commi successivi;
4. Con l'ausilio del GDL-Privacy e con la consulenza del DPO, sono predisposti e sottoscritti **appositi contratti o altri atti giuridici** che regolano i rapporti tra gli Enti "titolari" e i "responsabili del trattamento", per gli aspetti richiamati dall'art. 28 comma 3 del GDPR, cui si rimanda.
5. A seconda della natura e delle modalità del trattamento dei dati, gli stessi "responsabili dei trattamenti", secondo quanto specificato nei contratti stipulati, nonché con le procedure stabilite e comunicate dagli Enti titolari:
    - devono porre in essere adeguate misure tecniche ed organizzative per garantire la tutela dei dati personali secondo quanto stabilito nel GDPR, secondo gli stessi *principi di accountability cui sono tenuti gli Enti titolari;*
    - possono essere autorizzati a designare sub-responsabili autorizzati al trattamento dei dati;
    - devono tempestivamente comunicare agli Enti titolari, le violazioni dei dati personali (data breach) ai sensi di quanto previsto agli artt. 33 e 34 del GDPR,.
    - devono relazionare, con cadenza almeno annuale, dimostrando di avere previsto ed attuato adeguate misure e garanzie per la protezione dei dati personali trattati per conto degli Enti titolari.

Art.7 – Gruppo di lavoro privacy (GdL privacy)

1. Ai fini della gestione unitaria e del coordinamento generale di tutte le attività connesse all'attuazione del GDPR, l'Unione ed i Comuni si avvalgono di un "*gruppo di lavoro ('GdL privacy')* così composto, se non diversamente disposto dalla Giunta dell'Unione:
    - tre dirigenti o loro PO delegati;
    - un dipendente esperto in materia informatica;
    - un dipendente esperto in materia amministrativa;

2. I componenti del GdL-privacy vengono designati dalla Conferenza dei dirigenti, la quale individua altresì il personale di supporto per lo svolgimento delle ordinarie attività operative.

3. Il GdL Privacy - con il supporto e la collaborazione degli altri dirigenti e di tutti i responsabili dei servizi, nonché coinvolgendo il DPO, - svolge le seguenti attività di coordinamento generale per la materia dei trattamenti dei dati personali, che si elencano non esaustivamente:

a) indicazioni alla Giunta dell'Unione per i programmi/priorità di intervento per l'attuazione del GDPR, da sottoporre alla Conferenza dei dirigenti ed all'approvazione finale della Giunta dell'Unione;

b) raccolta e messa a disposizione degli interessati, degli elenchi degli incaricati/designati interni e dei responsabili esterni dei trattamenti dei dati (di cui agli artt. 6 e 8, il cui censimento ed aggiornamento resta a carico dei dirigenti e dei responsabili dei servizi);

c) indicazioni al servizio personale per la definizione di un programma permanente di informazione e formazione del personale, attinente all'attuazione del GDPR;

d) indicazioni per definire procedure e modulistica coerenti e uniformi per tutti gli Enti titolari, al fine di consentire la corretta attuazione del GDPR da parte di tutti i servizi (informative, formule per i consensi, comunicazioni, ecc.);

e) indicazioni ai dirigenti ed ai responsabili dei servizi per la tenuta ed aggiornamento dei seguenti "registri", necessari per l'attuazione del GDPR da parte degli Enti titolari, nonché per la dimostrabilità dell'effettiva attività svolta per garantire la tutela dei dati personali (principio di accountability):

- "registro per l'accountability" di cui all'art. 9;
- "registro dei trattamenti" di cui all'art. 12;

f) collaborazione al DPO/RPD per lo svolgimento delle sue verifiche sul rispetto, da parte dei servizi, delle norme e disposizioni in materia di trattamento dei dati personali.

Art.8 – Dipendenti designati/autorizzati per il trattamento dei dati personali nei diversi servizi

1. Tutti i dipendenti o altri soggetti che operano all'interno dei servizi dell'Unione e dei Comuni e che - in ragione dei compiti assegnati per le varie tipologie di trattamento – hanno accesso a dati personali, devono essere individuati ed istruiti, con modalità anche informali, dai dirigenti e responsabili di servizio cui sono assegnati e che hanno competenza per la loro gestione.
2. Tali soggetti sono autorizzati al trattamento dei dati personali, sotto l'autorità dei dirigenti e responsabili dei servizi in questione, i quali dovranno loro fornire istruzioni

adeguate per operare nel rispetto delle prerogative, modalità e/o limiti (stabiliti nell'Ente e nel settore/servizio) per la tutela dei dati personali.

3. L'individuazione dei "designati/autorizzati interni", non necessita di atti di nomina formale e deve risultare da appositi elenchi curati per ogni Settore e servizio dai rispettivi responsabili. Di norma essi corrispondono a quanto indicato nel registro dei trattamenti.

Art. 9 – Attuazione del principio di responsabilizzazione/accountability - Registro degli eventi (registro accountability)

1. Il GdL-privacy, i dirigenti ed i responsabili di servizio - ognuno per la loro competenza e secondo l'organizzazione interna stabilita - assicurano il **rispetto del principio di responsabilizzazione (accountability) di cui all'art. 5/2 del GDPR, comprovando le attività svolte per l'attuazione del GDPR,** mediante la tenuta di un apposito Registro (c.d. "Registro accountability"), nel quale annotano periodicamente le principali attività svolte ed eventi accaduti, in relazione alla gestione dei trattamenti dei dati personali.
2. Il registro è in formato elettronico, facilmente accessibile in modalità condivisa da tutti i soggetti chiamati alla sua compilazione ed aggiornamento.
3. Lo stesso registro è sempre accessibile direttamente da parte del DPO e, per suo tramite, dall'Autorità di controllo.

Art.10 – Misure per garantire la sicurezza dei trattamenti dei dati in ambito informatico

1. Le funzioni di "*amministratore dei sistemi informatici*", sono attribuite dal dirigente competente.
2. Lo stesso Dirigente, avvalendosi della struttura del Servizio informatico (SIA), provvede a:
   a) attuare e presidiare le **misure tecniche ed organizzative, in ambito ICT, per la sicurezza dei dati personali,** da individuare in relazione ai diversi trattamenti di dati personali, con la collaborazione dei competenti dirigenti e/o responsabili dei servizi. Tali misure di sicurezza, ai sensi dell'art. 32 del GDPR, possono comprendere, tra le altre:
      - pseudonimizzazione e cifratura dei dati personali;
      - sistemi/procedure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi;
      - sistemi/procedure per ripristinare tempestivamente la disponibilità ed accesso dei dati personali in caso di incidenti;

- sistemi/procedure per testare l'efficacia delle misure tecniche ed organizzative che garantiscono la sicurezza dei trattamenti dei dati;

b) fornire ai soggetti interni che sono autorizzati/designati per il trattamento di dati personali con strumenti informatici, periodiche indicazioni operative per la salvaguardia dei dati trattati;

c) relazionare annualmente alla Giunta dell'Unione ed al DPO sulle misure di sicurezza messe in atto per i trattamenti in ambito ICT, nonché sulla eventuale necessità di interventi e/o investimenti da programmare e finanziare;

d) fare risultare tutte le attività svolte per la sicurezza dei dati in ambito ICT, nel "Registro accountability" di cui all'art. 9.

3. Le stesse misure di sicurezza vengono indicate per ciascun trattamento nel "Registro dei trattamenti" di cui all'art. 12, potendosi disporre la non pubblicizzazione, qualora sia necessario mantenerle riservate.

4. La valutazione dei rischi e le conseguenti misure di sicurezza relative agli aspetti diversi dall'informatica/ICT (conservazione fascicoli, gestione archivi cartacei, ecc), restano nella competenza dei dirigenti e responsabili di servizi, competenti nei diversi settori/servizi.

5 Qualunque incidente di sicurezza che comporti anche una violazione di dati personali deve essere tempestivamente segnalato e trattato, con le modalità previste dalla procedura di gestione dei data breach.

Art.11 – Responsabile della protezione dei dati (DPO).

1. **Il responsabile della protezione dei dati (DPO -**"*data protection officer*") è designato dagli Enti titolari - in forma unica associata per l'Unione e per i Comuni aderenti - tenendo conto di quanto previsto dagli artt. 37-38-39 del GDPR, nonché dalle "linee guida" del Comitato europeo per la privacy *(WP 243 - Linee-guida sui DPO)* e dal "Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico" del Garante per la Protezione dei dati Personali (Provvedimento del 29 aprile 2021);

2. Qualora la designazione del DPO, non potendo avvenire tra il personale interno, verta su un soggetto esterno, le modalità di affidamento dell'incarico sottostanno alla normativa in materia di appalti ("contratto di servizi").

3. Il DPO, interno o esterno, **opera in autonomia ed indipendenza** non potendo ricevere alcuna istruzione. Egli si relaziona direttamente con il vertice politico e gestionale degli Enti titolari dei trattamenti dei dati.

4. Il DPO - con riferimento all'insieme dei trattamenti di dati effettuati dall'URF e dai Comuni aderenti - svolge i compiti previsti dall'art. 39 del GDPR e, in particolare:

a) **informare e fornire consulenza** al titolare e/o ai responsabili del trattamento, nonché a tutti coloro che eseguono il trattamento dei dati, in merito agli obblighi derivanti dal GDPR, relativi alla protezione dei dati;

b) **sorvegliare l'osservanza del GDPR** e delle altre disposizioni nazionali, relative alla protezione dei dati, nonché delle politiche sulla protezione dei dati personali adottate dal titolare e/o dai responsabili del trattamento, compresi l'attribuzione delle responsabilità, la protezione dei dati personali, 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 (DPIA) e sorvegliarne lo svolgimento ai sensi dell'*art.35 del GDPR*;

d) **cooperare con il Garante nazionale** per la protezione dei dati personali e fungere da suo punto di contatto per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'*art. 36 GDPR*, ed effettuare, se del caso, consultazioni.

5. **Gli interessati possono contattare il DPO** per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.
6. Il DPO è tempestivamente e adeguatamente coinvolto dal GdL-privacy di cui all'art. 7, dai dirigenti e dai responsabili di servizio competenti, per tutte le questioni riguardanti la protezione dei dati personali oggetto di trattamento negli Enti.
7. **Gli Enti titolari sostengono** il DPO nell'esecuzione dei predetti compiti, fornendogli le risorse e gli strumenti necessari per assolvere tali compiti, nonché per mantenere la propria conoscenza specialistica.
8. Il DPO, qualora interno, se non dotato di autonome risorse dalla Giunta dell'Unione, è supportato, per lo svolgimento dei suoi compiti, da uno staff composto da dipendenti dell'Unione individuati in accordo con la Conferenza dei dirigenti, in cui siano presenti almeno:
   a) un dipendente esperto in materia informatica;
   b) un dipendente esperto in materia amministrativa;
   c) un dipendente con funzioni di segreteria operativa;
9. Il DPO è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti. Egli ha l'obbligo di astenersi nel caso sussistano condizioni di conflitto di interesse.

Art.12 – Registro dei trattamenti (art. 30 GDPR)

1. L'Unione ed i Comuni istituiscono un registro unico delle attività di trattamento di dati personali svolti sotto la propria responsabilità, in forma scritta, anche in formato elettronico, contenente le informazioni di cui all'*art.30 del GDPR.*

2. **Il "registro dei trattamenti"** - il cui schema viene approvato dalla Giunta dell'Unione su proposta del GdL privacy e previo parere del DPO - è **unico per l'Unione e per i Comuni** aderenti, in ragione della loro contitolarità del trattamento di dati, nonché dell'unica struttura amministrativa di cui essi sono dotati;

3. I dirigenti ed i Responsabili di servizio dell'Unione - secondo le rispettive competenze stabilite all'interno dei Settori – completano ed aggiornano il "registro dei trattamenti", con riferimento ai trattamenti dei rispettivi servizi, con il supporto del GdL-privacy, nonché con la consulenza del DPO;

4. Gli aggiornamenti del "registro dei trattamenti" devono avvenire solo in ragione di eventuali modifiche delle attività di trattamento dei dati personali (da fare sempre corrispondere a quanto descritto nel registro);

5. Il "*registro dei trattamenti"* è sempre accessibile direttamente da parte del DPO e, per suo tramite, dall'Autorità di controllo.

Art.13 – Valutazione di impatto sulla protezione dei dati (DPIA)

1. L'Unione ed i Comuni - in attuazione dell'art. 35 del GDPR, con riguardo alle tipologie di trattamento indicate dall'Autorità di controllo, con la consulenza del DPO – individuano tra i trattamenti di cui sono titolari quelli che presentano un potenziale di rischio elevato per i diritti delle persone.

2. Per gli stessi "trattamenti a rischio", vengono effettuate apposite *"valutazioni di impatto sulla protezione dei dati" (DPIA),* con le modalità descritte all'*art.35 del GDPR*, attraverso anche gli strumenti messi a disposizione dall'Autorità garante-privacy.

3. Le DPIA sono predisposte e sottoscritte, in formato digitale, a cura del dirigente e/o del responsabile di servizio, competente per quel trattamento, con la consulenza del DPO. Esse si basano sulla valutazione dei pericoli per la riservatezza e per i diritti fondamentali della persona e contengono la previsione delle azioni e delle misure di sicurezza e di garanzia per il miglioramento delle condizioni di trattamento e per la mitigazione del rischio.

Art.14 Segnalazione delle violazione dei dati personali (data breach).

1. Ai sensi dell'*art.4/12 del GDPR*, costituisce "violazione dei dati personali" una *violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la*

perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. La segnalazione della violazione deve essere effettuata - nella stessa giornata della sua scoperta - **da parte del dirigente e/o del responsabile del servizio competente, nei confronti del GdL-privacy e del DPO**, al fine di consentire agli stessi la valutazione sulla gravità della violazione e l'eventuale notifica all'Autorità di controllo ai sensi di quanto previsto dagli *artt 33-34 del GDPR* , nel rispetto del termine di 72 ore dal momento in cui si è venuti a conoscenza della violazione stessa.

3. Nella segnalazione, da formulare per iscritto, deve essere fatta una dettagliata descrizione del tipo di violazione e delle circostanze che l'hanno caratterizzata, del tipo di trattamento interessato, dei dati e delle persone fisiche interessate ed ogni altro elemento che possa far valutare i rischi che corrono i diritti e le libertà delle persone coinvolte.

4. Il DPO valutato - con il supporto del personale di staff e del GdL privacy - il tipo di violazione e la gravità delle possibili conseguenze, supporta il Titolare nella notifica della violazione all'Autorità di controllo e, ove previsto, agli interessati dal trattamento (persone a cui si riferiscono i dati oggetto di violazione). Egli attiva anche le verifiche in merito alle cause che hanno determinato la violazione stessa.

5. Anche nel caso di mancata notifica all'Autorità di controllo per assenza di rischi per i diritti e le libertà delle persone fisiche, la violazione dei dati è riportata nel registro delle attività di cui al precedente art. 9.

Art.15 – Informativa agli interessati.

1. I dirigenti e/o i responsabili di servizio – con il supporto del GdL-privacy e con la consulenza del DPO – redigono, per le unità organizzative di competenza, le informative riguardanti i trattamenti dei dati, da mettere a disposizione degli interessati, sia nel caso abbiano fornito direttamente i dati (art. 13 GDPR), sia nel caso non li abbiano forniti direttamente (*art.14 GDPR).*

2. Le informative vengono rese in una forma e con un linguaggio concisi, trasparenti, intelligibili e facilmente accessibili.

3. Le predette informative sui trattamenti possono essere messe a disposizione degli interessati tramite:

- avvisi generali sul sito web degli Enti;
- avvisi generali da mostrare all'interno degli uffici in cui avviene il contatto con gli interessati;
- avvisi generali da affiggere all'esterno degli uffici;

- all’interno della modulistica/dei provvedimenti/dei contratti;
- con comunicazioni mirate agli interessati;
- con altri mezzi comunicativi individuati dal dirigente per ottemperare alle finalità di cui alle predette norme.

4. La scelta dei mezzi attraverso cui rendere l’informativa viene valutata anche sulla base della tipologia di utenza, del numero di utenti da informare, delle caratteristiche dei trattamenti dei dati.

5. I dirigenti ed i responsabili dei servizi si accertano della corretta formazione/istruzione dei dipendenti che si trovano in uffici a contatto diretto con il pubblico i quali - essendo addetti alla raccolta dei dati personali direttamente dagli interessati - devono essere in grado di dare anche verbalmente adeguate informazioni sulle finalità, modalità e tipologie di trattamento dei dati personali, a richiesta degli stessi interessati;

Art.16 – Esercizio dei diritti

1 Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del GDPR.

2 Se ritiene che il trattamento dei dati personali non sia conforme alle disposizioni vigenti ovvero se la risposta ad un’istanza con cui esercita uno o più dei diritti di cui al comma 1, non perviene nei tempi indicati o non è soddisfacente, l’interessato può rivolgersi all'Autorità Giudiziaria o all’Autorità di controllo (Garante per la protezione dei dati personali), in quest'ultimo caso mediante un reclamo ai sensi dell’art. 77 del GDPR.

3 L'istanza può essere riferita a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali, comunque trattati, ed è presentata all’Unione o ai Comuni, titolari dei dati, senza formalità (es. posta elettronica, lettera raccomandata, etc.), fatte salve le limitazioni di cui agli artt. 2-undecies e 2-duodecis del D.LGS 196/2003 e le altre limitazioni previste dalla legge.

4 L’istanza scritta è indirizzata all’Unione o ai Comuni, titolari dei dati, tramite il RPD/DPO, ai dirigenti e ai Responsabili di servizio dove sono trattati i dati. Qualora il trattamento coinvolga più Servizi, il Dirigente o il Responsabile ricevente l’istanza ne dà comunicazione agli altri Dirigenti/Responsabili che detengono i dati personali dell’interessato.

5 Se il trattamento è effettuato da soggetti terzi per conto dell'Unione o dei Comuni, sull’istanza è competente a rispondere il Dirigente che ha provveduto alla nomina del fornitore del servizio.

6 Il riscontro all’istanza presentata viene fornito, senza ingiustificato ritardo, entro 30 giorni dalla data di ricezione della stessa, anche nei casi di diniego.

7 Se le operazioni necessarie per il riscontro sono complesse o vi è una particolare e comprovata difficoltà, il termine dei 30 giorni può essere esteso fino a 2 mesi, non ulteriormente prorogabili. Di tale proroga viene data informazione all'interessato entro 20 giorni dalla ricezione dell'istanza.