



**Regolamento per l'attuazione
del Regolamento UE 2016/679 relativo
alla protezione delle persone fisiche
con riguardo al trattamento dei dati personali**

approvato con delibera dell'Assemblea Consortile n. 25 del 27/09/2024

INDICE

Art. 1 - Oggetto

Art. 2 - Titolare del trattamento

Art. 3 - Finalità del trattamento

Art. 4 - Nomina di soggetti delegati dal Presidente: i titolari di Posizioni Organizzative

Art. 5 - Responsabile della protezione dati

Art. 6 - Sicurezza del trattamento

Art. 7 - Registro delle attività di trattamento

Art. 8 - Registro delle categorie di attività trattate

Art. 9 - Valutazione d'impatto sulla protezione dei dati

Art. 10 - Violazione dei dati personali

Art. 11 - Rinvio

Allegati

A) registro delle attività di trattamento ai sensi dell'art. 30 del Regolamento UE 2016/679

Art. 1 Oggetto

1. Il presente Regolamento ha per oggetto misure procedurali 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 "GDPR", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, in questo Ente.

Art.2 Titolare del trattamento

1. L'Ente, rappresentato ai fini previsti dal GDPR dal Presidente pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Presidente può delegare le relative funzioni al Direttore/Segretario/P.O. in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: 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 GDPR.

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 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

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:

a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. 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 deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, GDPR, considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

6. Il Titolare, inoltre, provvede a:

~~a) designare i Responsabili del trattamento nelle persone dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture in cui si articola l'organizzazione consortile, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;~~

a) nominare il Responsabile della protezione dei dati;

b) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione consortile, relativamente alle banche dati gestite da soggetti esterni all'Ente in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

c) predisporre l'elenco dei titolari di Posizioni Organizzative delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Ente da enti ed organismi statali o regionali, 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 GDPR. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, 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 GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo

può individuare un punto di contatto comune per gli interessati.

8. L'Ente 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 GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei titolari di Posizioni Organizzative.

Art.3 Finalità del trattamento

1. I trattamenti sono compiuti dall'Ente 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:

- 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 all'Ente in base alla vigente legislazione.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

b) l'adempimento di un obbligo legale al quale è soggetto l'Ente. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto con soggetti interessati;

d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art.4 Nomina di soggetti delegati dal Presidente: i titolari di Posizioni Organizzative

1. Il Presidente *pro tempore* può provvedere a designare il Direttore del Consorzio Rifiuti del VCO o il Segretario Generale quali incaricati di Posizioni Organizzative.

2. I dipendenti dell'Ente, Titolare del trattamento, sono nominati autorizzati al trattamento, con lettera di autorizzazione ex art. 29 GDPR, direttamente dal Presidente oppure dai titolari di Posizioni Organizzative di cui al precedente punto. Nell'atto di incarico, nel quale sono tassativamente disciplinati:

- 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;

- le disposizioni del Titolare del Trattamento alle quali si devono attenere al fine di un corretto e lecito trattamento dei dati trattati;

- gli obblighi ed i diritti del Titolare del trattamento.

3. Il Titolare può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di Responsabili del trattamento, forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del Responsabile per la Protezione dei Dati (RPD), se previsto come obbligo normativo;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad 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 Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art.5 Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato nella figura unica di un dipendente di ruolo dell'ente di qualifica non inferiore alla cat. D, 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 consortile. Il Titolare e le P.O. provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

Nel caso in cui il RPD non sia il segretario o un dipendente dell'ente, l'incarico può essere affidato ad un soggetto esterno, persona fisica o giuridica, selezionata mediante procedura ad evidenza pubblica 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 alle P.O.

E' inoltre possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più ente mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267.

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare e ai titolari di Posizioni Organizzative nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o alle P.O. i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e delle P.O.

Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e delle P.O.;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dalle P.O.;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le

conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dalle P.O. al Garante;

f) l'eventuale tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o le P.O. si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

2. Il Titolare e le P.O. assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

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. In tal senso il RPD:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed alle P.O.

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e 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 in relazione alle dimensioni organizzative dell'ente:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;

- le P.O.;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il Titolare e le P.O. forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/ P.O. e del Consiglio di Amministrazione, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;

- tempo sufficiente per l'espletamento dei compiti affidati al RPD;

- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);

- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;

- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

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 dalle P.O. per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - o suo delegato - o alle P.O.

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed alle P.O.

Art.6 Sicurezza del trattamento

1. L'Ente e ciascun Responsabile del trattamento mettono 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 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 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.
3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun titolare di una Posizione Organizzativa:
 - 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. L'Ente e ciascuna P.O. si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi ed i dati di contatto del Titolare, del o delle P.O. e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Ente, 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 seguenti informazioni:
 - a) il nome ed i dati di contatto dell'Ente, del Presidente e/o del suo Delegato ai sensi del precedente art.2, eventualmente del Contitolare del trattamento, del RPD;
 - b) le finalità del trattamento;
 - 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) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.
2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa dell'Ente in forma telematica/cartacea, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

4. Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo art. 8, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema allegato C al presente Regolamento. In tal caso, il Titolare delega la sua tenuta alle P.O. di cui al precedente art. 4 o, comunque, ad un solo titolare di Posizione Organizzativa, ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art.8 Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun soggetto di cui al precedente art. 4, reca le seguenti informazioni:

- a) il nome ed i dati di contatto del Titolare del trattamento e del RPD;
- b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
- c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il registro è tenuto dal Titolare del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato B al presente regolamento.

3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

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'art. 35, pp. 4-6, RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, 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, 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 Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Ente.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA 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.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

 se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;

 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;

 se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

 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 necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. 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:

_ delle finalità specifiche, esplicite e legittime;

_ della liceità del trattamento;

_ dei dati adeguati, pertinenti e limitati a quanto necessario;

_ del periodo limitato di conservazione;

_ delle informazioni fornite agli interessati;

_ del diritto di accesso e portabilità dei dati;

_ del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;

_ dei rapporti con i responsabili del trattamento;

_ delle garanzie per i trasferimenti internazionali di dati;

_ 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.

8. Il Titolare 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.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy 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.

10. 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.

(eventuale) 11. E' 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.

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 dall'Ente.

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.

Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, 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 conseguentemente 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 GDPR, 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 GDPR.

Art.11 Rinvio

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

ALLEGATI

A) Registro attività di trattamento

B) Registro categorie di attività di trattamento

C) Registro unico dei trattamenti

GLOSSARIO REGOLAMENTO

Ai fini della proposta di Regolamento consortile, si intende per:

❖ Titolare del trattamento

l'autorità pubblica (l'Ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

❖ Soggetti titolari di Posizioni Organizzative

il direttore o il Segretario Generale, nominati dal Presidente quali titolari di Posizione organizzativa

❖ Responsabile del Trattamento

soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.

❖ Soggetto autorizzato al trattamento

il dipendente della struttura organizzativa dell'Ente, incaricato dal Titolare del trattamento o dai titolari di Posizioni Organizzative, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali).

❖ Responsabile per la protezione dati – RPD

il dipendente della struttura organizzativa dell'Ente, il professionista privato o impresa esterna, incaricati dal Titolare o dalla P.O.

❖ Registri delle attività di trattamento

elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dai titolari di Posizioni Organizzative secondo le rispettive competenze.

❖ DPIA - Data Protection Impact Assessment” - “Valutazione d’impatto sulla protezione dei dati

è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

❖ Garante Privacy

il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.

GLOSSARIO REGISTRI

Ai fini delle proposte dei registri, si intende per:

❖ Categorie di trattamento

Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

❖ Categorie di dati personali

Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.

Dati inerenti lo stile di vita

Situazione economica, finanziaria, patrimoniale, fiscale.

Dati di connessione: indirizzo IP, login, altro.

Dati di localizzazione: ubicazione, GPS, GSM, altro.

❖ Finalità del trattamento

Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri:

funzioni amministrative inerenti alla popolazione ed il territorio, nei settori organici dei servizi alla persona, 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 all'Ente.

Adempimento di un obbligo legale al quale è soggetto l'Ente. Esecuzione di un contratto con i soggetti interessati. Altre specifiche e diverse finalità.

❖ Misure tecniche ed organizzative

Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.

Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.

Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.

Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

❖ Dati particolari

Dati inerenti all'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale, dati genetici e biometrici, dati relativi a condanne penali.

❖ Categorie interessati

Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

❖ Categorie destinatari

Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO EX ART. 30 GDPR

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO EX ART. 30 GDPR												
Titolare del trattamento dei dati						Responsabile della protezione dei dati - DPO						
Struttura			Contatti			Struttura			Contatti			
Consorzio Rifiuti del Verbano Cusio Ossola			e-mail: info@consorziorifiutivco.it			Labor Service S.r.l.			privacy@labor-service.it			
Via Olanda, 57			PEC: protocollo@pec.consorziorifiutivco.it			Via Righi, 29			pec@pec.labor-service.it			
28922 - Verbania (VB)			Tel 0323/507071			28100 Novara			Tel. 0321/1814220			
P.IVA 02235970031			Fax 0323/557514			P. IVA 02171510031						
nr.	Settore	Attività	Finalità	Base giuridica	Categoria degli interessati	Categoria di dati	Destinatari	Trasferimento dati Extra UE	Periodo di conservazione	Misure di sicurezza tecniche	Misure di sicurezza organizzative	Contitolari
1	SERVIZIO PRINCIPALE: AMBIENTE E NETTEZZA URBANA	Governo e coordinamento, in forma associata, dei servizi di igiene urbana, assicurando la realizzazione e gestione delle attività di spazzamento stradale, dei conferimenti separati, dei servizi di raccolta differenziata e di raccolta del rifiuto indifferenziato.	Adempimento di un obbligo previsto dalla legge (Legge regionale n°24/2002); governo del territorio sotto il profilo della salvaguardia della salute pubblica (es. Art. 13 TUEL)	Adempimento di un obbligo di legge; esecuzione di un compito di interesse pubblico (art. 6, lett. c, e GDPR)	Cittadini residenti e non, liberi professionisti, rappresentanti di imprese, altri enti e società	Dati personali comuni: dati anagrafici; Dati giudiziari ex art. 10 GDPR	Titolari autonomi: Ministero dei Lavori Pubblici, Regione, ARPAL, ASL, altri Enti pubblici e società pubbliche e private di gestione di servizi pubblici	NO	Conservazione permanente	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
2	RAGIONERIA-ECONOMATO	Gestione dell'attività finanziaria corrente dell'Ente: impegni di spesa, registrazioni contabili, mandati di pagamento, liquidazioni, fatture elettroniche.	Gestione finanziaria e contabile dell'ente	Adempimento di un obbligo di legge, esecuzione del contratto di servizio (art. 6, lett. b, c GDPR)	Cittadini, liberi professionisti, rappresentanti di imprese e fornitori in genere	Dati personali comuni: anagrafici; Dati particolari ex art. 9 GDPR: relativi alla salute Dati giudiziari ex art. 10 GDPR	Titolari autonomi: Cassa Depositi e Prestiti e altri istituti di credito privati, Ministero dell'Economia e delle Finanze, Banca d'Italia, Agenzia delle Entrate, Tesoreria Provinciale, Revisore del conto, Tesoriere comunale Responsabili del trattamento ex art. 28	NO	Permanente, previo sfolgimento (V. piano di conservazione: Titolo IV punto 2)	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
3	TRIBUTI	Attività di gestione delle entrate comunali dipendenti TARI dei Comuni di Crevaladossola e Stresa. Dal 1 gennaio 2020, il C.R del VCO non svolge più questa attività a favore di tali comuni, che hanno preso l'intera titolarità dell'incarico. Tuttavia, il C.R. del VCO continua a gestire le situazioni di morosità per il solo Comune di Stresa.	Gestione entrate comunali	Adempimento di un obbligo di legge; esecuzione di un compito di interesse pubblico (art. 6, lett. c, e GDPR)	Cittadini residenti e non, rappresentanti di imprese, altri enti con sede sul territorio	Dati personali comuni: anagrafici; Dati particolari ex art. 9 GDPR: relativi alla salute per riduzioni Dati giudiziari ex art. 10 GDPR	Titolari autonomi: Agenzia del Territorio, Agenzia delle Entrate, Guardia di Finanza; Responsabili del trattamento ex art. 28 GDPR	NO	Fascicoli personali dei contribuenti comunali 10 anni dopo la cancellazione del contribuente dai ruoli; Ruolo 10 anni. I dati vengono conservati fino al termine delle procedure.	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
4	RISORSE UMANE	Gestione rapporti di lavoro	Instaurazione e gestione rapporti di lavoro dipendente di qualunque tipo e altre forme di impiego che non comportano costituzione di rapporto di lavoro subordinato	Adempimento di un obbligo di legge; esecuzione di un contratto (di lavoro) di cui l'interessato è parte (art. 6, lett. b, c GDPR)	Dipendenti dell'Ente e famigliari	Dati personali comuni: anagrafici; di contatto, economici, sociali Dati particolari ex art. 9 GDPR: relativi alla salute, iscrizione sindacale Dati giudiziari ex art. 10 GDPR	Titolari autonomi: INAIL, INPS, ASL, autorità pubbliche, medico competente Responsabili del trattamento ex art. 28 GDPR	NO	Permanente previo sfolgimento da eseguire seguendo la tempistica prevista per le singole classi (V. piano di conservazione: Titolo III punto 1)	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
5	ARCHIVIO PROTOCOLLO	Registrazione atti, provvedimenti e comunicazioni in arrivo, in partenza e interne all'Ente, e assegnazione a servizi e uffici per espletamento procedimenti e pratiche di	Presa in carico e trasmissione da parte dell'Ente di atti e comunicazioni anche con valore giuridico	Adempimento di un obbligo di legge (art. 6 lett. c GDPR)	Cittadini, residenti e non, rappresentanti di imprese, dipendenti di altri enti pubblici	Contenuti nell'atto protocollato	Responsabili del trattamento ex art. 28 GDPR	NO	Permanente	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
6	SEGRETERIA	Documentazione dell'attività istituzionale e degli organi del Consorzio: stesura e conservazione della documentazione formalizzata dall'Ente (es. delibere, decreti, determinazioni che comportano la gestione di beni o di risorse finanziarie)	Gestione della documentazione amministrativa e relativa pubblicazione sul sito istituzionale	Adempimento di un obbligo di legge (art. 6 lett. c GDPR)	Cittadini, persone fisiche e rappresentanti di persone giuridiche in generale	Dati personali comuni: anagrafici e di contatto; Dati giudiziari ex art. 10 GDPR: autodichiarazione condanne reati contro PA	Titolari autonomi: Autorità competenti nei casi previsti da norme di legge; diffusione attraverso pubblicazione salvo Omissis; Responsabili del trattamento ex art. 28 GDPR	NO	Permanente	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
7	SEGRETERIA	Attività relativa alla gestione delle richieste di accesso agli atti amministrativi	Adempimento di un obbligo previsto dalla legge (legge 241/1990, d.lgs. 33/2013)	Adempimento di un obbligo di legge; esecuzione di un compito di interesse pubblico (art. 6, lett. c, e GDPR)	Cittadini, persone fisiche e rappresentanti di persone giuridiche	Dati personali comuni: anagrafici e di contatto	Titolari autonomi: Difensore civico regionale, Garante della Privacy, Tribunale amministrativo regionale; Responsabili del trattamento ex art. 28 GDPR	NO	Permanente	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO EX ART. 30 GDPR

Titolare del trattamento dei dati							Responsabile della protezione dei dati - DPO					
Struttura			Contatti				Struttura			Contatti		
Consorzio Rifiuti del Verbano Cusio Ossola			e-mail: info@consorziorifiutivco.it				Labor Service S.r.l.			privacy@labor-service.it		
Via Olanda, 57			PEC: protocollo@pec.consorziorifiutivco.it				Via Righi, 29			pec@pec.labor-service.it		
28922 - Verbania (VB)			Tel 0323/507071				28100 Novara			Tel. 0321/1814220		
P.IVA 02235970031			Fax 0323/557514				P. IVA 02171510031					
nr.	Settore	Attività	Finalità	Base giuridica	Categoria degli interessati	Categoria di dati	Destinatari	Trasferimento dati Extra UE	Periodo di conservazione	Misure di sicurezza tecniche	Misure di sicurezza organizzative	Contitolari
8	SEGRETERIA	Gestione amministrativa dei membri del Consorzio: nomine, registrazione presenze, revoca	Adempiere correttamente gli obblighi di legge	Adempimento di un obbligo di legge; esecuzione di un compito di interesse pubblico (art. 6, lett. c, e GDPR)	Membri del Consiglio di Amministrazione	Dati personali comuni: anagrafici	Non ci sono destinatari	NO	Permanente	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
9	SEGRETERIA	Annotazione, in apposito registro, dei reclami avanzati dagli utenti per disservizi di raccolta	Migliorare il servizio offerto dal Titolare	Perseguimento di un interesse pubblico (art. 6 lett e GDPR)	Cittadini, persone fisiche e rappresentanti di persone giuridiche	Dati personali comuni: anagrafici e di contatto;	Non ci sono destinatari	NO		Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
10	GARE E APPALTI PUBBLICI	Manifestazione di interesse per la partecipazione alle gare di appalto di servizi relativamente ad un determinato piano d'ambito; successiva offerta tecnico-economica da parte dei candidati; provvedimento finale di incarico per la fornitura del servizio	Adempimento di tutti gli obblighi imposti dal Codice degli appalti	Esecuzione di un contratto e di misure precontrattuali di cui l'interessato stesso è parte; adempimento di un obbligo di legge; esecuzione di un compito di interesse pubblico	Cittadini, persone fisiche e rappresentanti di persone giuridiche	Dati personali comuni: anagrafici e di contatto; Dati giudiziari ex art. 10 GDPR: autodichiarazione condanne reati contro PA	Cittadinanza, ANAC	NO	Permanente	Vedi foglio "MISURE TECNICHE"	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
11	SEGRETERIA	Gestione dei dati relativi al sito internet aziendale e richieste di contatto	Sicurezza dei dati; controllo dati di navigazione; gestione richieste di contatto	Art. 6, lett. f) GDPR: legittimo interesse del Titolare	Utenti del sito	Dati personali comuni: dati di contatto; dati di navigazione	Responsabili del trattamento ex art. 28 GDPR	NO	2 anni	Vedi foglio "MISURE TECNICHE"; Sicurezza del sito internet; Privacy Policy e Cookie policy conformi	Persone che trattano i dati autorizzate con lettera di incarico e istruzioni; contratti ex art. 28 GDPR; informative; regolamento sul trattamento dei dati adottato dall'ente; nomina del DPO	NO
11	UFFICIO SEGRETERIA (RPCT)	Segnalazioni whistleblowing	Ricezione, raccolta, gestione e conservazione di segnalazione di un presunto illecito per la prevenzione di illeciti a danno dell'interesse pubblico come stabilito da legge (c.d. Whistleblowing)	Art. 6, lett. c) ed e), GDPR: L. 6 novembre 2012, n. 190; D.Lgs. 24 del 10 marzo 2023; Linee Guida in materia di Whistleblowing pubblicate da ANAC	Soggetto segnalante (es. dipendenti, lavoratori autonomi, professionisti; volontari, tirocinanti); soggetti segnalati; altri soggetti che possono riferire sull'oggetto della segnalazione o legati al segnalante (es. facilitatori)	Personali comuni (anagrafici, di contatto ed altri dati desunti dalla segnalazione); particolari e giudiziari (reati)	Titolari autonomi: Autorità giudiziaria; Corte dei Conti; ANAC Responsabile del trattamento ex art. 28 GDPR: fornitore della piattaforma volta alla ricezione e conservazione delle segnalazioni	NO	Conservazione per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione	Lettera di autorizzazione con specifiche istruzioni per l'RPCT e per altri dipendenti preposti all'attività; formazione specifica alle persone fisiche preposte alla ricezione/gestione; canali di segnalazione interni previsti dall'ente e adeguati al mantenimento della riservatezza dell'identità delle persone fisiche interessate (piattaforma digitale protetta da crittografia e credenziali di accesso riservate); trasmissione dell'atto organizzativo alle organizzazioni/sigle sindacali nazionali; messa a disposizione dell'Informativa privacy ex art. 13 GDPR agli interessati; presenza di un contratto di nomina per i fornitori della piattaforma di ricezione delle segnalazioni.	Lettera di autorizzazione con specifiche istruzioni per l'RPCT e per altri dipendenti preposti all'attività; formazione specifica alle persone fisiche preposte alla ricezione/gestione; canali di segnalazione interni previsti dall'ente e adeguati al mantenimento della riservatezza dell'identità delle persone fisiche interessate (piattaforma digitale protetta da crittografia e credenziali di accesso riservate); trasmissione dell'atto organizzativo alle organizzazioni/sigle sindacali nazionali; messa a disposizione dell'Informativa privacy ex art. 13 GDPR agli interessati; presenza di un contratto di nomina per i fornitori della piattaforma di ricezione delle segnalazioni.	NO

NUM	MISURE di SICUREZZA
A	Adozione delle misure di sicurezza previste dal D.Lgs 81/2008
B	Adozione di procedure per le copie di sicurezza ed il ripristino della disponibilità dei dati
C	Aggiornamento periodico dei programmi antivirus
D	Aggiornamento degli apparati hardware e software
E	Aggiornamento periodico delle credenziali di autenticazione assegnate, ad uso esclusivo, ad ogni operatore i quali sono tenuti al segreto e alla custodia delle credenziali di autenticazione
F	Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incaricato
G	Assegnazione e gestione dei profili di autorizzazione con verifica periodica dei requisiti
H	Formazione sugli aspetti principali della disciplina della privacy
I	Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento senza l'ausilio di strumenti elettronici
L	Presenza di un contratto di assistenza per i software gestionali
M	Sistema di protezione dei dati trasmessi: crittografia e/o cifratura
N	Archivi dotati di serratura