



**Strada J.F. Kennedy, 504
15122 Castelceriolo (AL)
tel. 0131586010 – fax 0131585963
PEC: aral-spa@legalmail.it
P.I. 02021620063**

**REGOLAMENTO PER L'ATTUAZIONE DEL RGPD (REGOLAMENTO GENERALE
PROTEZIONE DATI - REG. UE 2016/2017) RELATIVO ALLA PROTEZIONE DELLE
PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI**

- Art. 1 - Oggetto
- Art. 2 - Definizioni
- Art. 3 - Titolare del trattamento
- Art. 4 - Finalità del trattamento dati personali
- Art. 5 - Designati/autorizzati
- Art. 6 - Responsabile esterno
- Art. 7 - Responsabile Protezione Dati
- Art. 8 - Sicurezza del trattamento
- Art. 9 - Registro unico delle attività di trattamento
- Art. 10 - Valutazioni d'impatto sulla protezione dei dati
- Art. 11 - Violazione dei dati personali ("data breach")
- Art. 12 - Valutazione d'impatto sulla protezione dei dati
- Art. 13 - Videosorveglianza
- Art. 14 - Cessazione del trattamento dei dati
- Art. 15 - Comunicazione
- Art. 16 - Rinvio

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 Generale Protezione Dati (di seguito indicato con "RGPD") e della normativa interna, relative alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'ambito della complessiva attività svolta da ARAL Azienda Rifiuti Alessandrina S.p.A.

Art. 2 Definizioni

Ai fini del presente regolamento s'intende per:

- 1) "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) "archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- 4) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 5) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- 6) "destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali;
- 7) "terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 8) "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- 9) "violazione dei dati personali": la 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;
- 10) "dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Art. 3

Titolare del trattamento

1. ARAL Azienda Rifiuti Alessandrina S.p.A., nella persona del 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”)

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dalla normativa europea: 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 a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.

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 dalla normativa europea, 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 e di bilancio, 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 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall’art. 14 RGPD, qualora i dati personali non siano 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 della normativa europea, considerati 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:

a) designa per specifici compiti e funzioni i dirigenti e preposti alle strutture in cui si articola l’organizzazione societaria;

b) nomina il Responsabile della protezione dei dati;

Art. 4

Finalità del trattamento dati personali

1. I trattamenti relativi ai dati personali sono effettuati da ARAL Azienda Rifiuti Alessandrina S.p.A. per le seguenti finalità:

a) l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri, riconducibile, in termini generali, a tutte le operazioni di recupero e smaltimento rifiuti poste in

capo alla Società, compresa la gestione dei siti di discarica e dell'impianto di tmb, oltre alle attività ad esse subordinate, funzionali o collaterali;

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

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

2. I trattamenti di particolari categorie di dati sono compiuti, se previsti dal diritto dell'Unione Europea o da disposizione di legge, per motivi di interesse pubblico rilevante, proporzionato alla finalità perseguita, come individuati dalla legge

3. Con riguardo ai dati relativi a condanne penali o reati, il trattamento è consentito solo se autorizzato da norma di legge.

4. Fuori dai casi previsti dal comma 1, il trattamento è ammesso solo se l'interessato presta il proprio consenso.

5. Ai sensi dell'art. 5 del RGPD, ARAL Azienda Rifiuti Alessandrina S.p.A.:

a) tratta i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato (secondo i principi di liceità, correttezza e trasparenza”);

b) raccoglie i dati personali per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (secondo il principio di limitazione della finalità”);

c) tratta solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (secondo il principio di “minimizzazione dei dati”);

d) tratta solo dati personali esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (secondo il principio di “esattezza”);

e) conserva i dati personali in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (secondo il principio della “limitazione della conservazione”);

f) tratta solo dati personali in maniera da garantire un'adeguata sicurezza degli stessi, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (secondo il principio di “integrità e riservatezza”).

Art. 5 Designati/autorizzati

1. Il Designato (responsabile del trattamento dei dati personali acquisiti mediante il sistema di videosorveglianza attivato presso il Complesso IPPC “impianto di tmb” sito in Comune di Castelceriolo e presso il complesso IPPC “discarica per rifiuti non pericolosi” sita in Comune di Solero) è il direttore pro-tempore, individuato con apposito atto del titolare ai sensi dell'art. 2-

quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) del Codice in materia di protezione dei dati personali approvato con D.lgs. 196/2003 e ss.mm.ii.

2. A Dirigenti e preposti (“Designati”) possono essere attribuiti specifici compiti e funzioni connessi al trattamento dei dati personali esistenti nell’articolazione organizzativa di rispettiva competenza.

3. I dipendenti della Società sono autorizzati dal Designato competente al trattamento dei dati riferiti alla struttura di riferimento come individuati nel rispettivo registro dei trattamenti, con il 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;
- gli obblighi ed i diritti del Titolare del trattamento
- le misure di sicurezza in rapporto ai rischi.

Ai dipendenti autorizzati verranno fornite specifiche istruzioni.

4 Il Designato provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidati dal Titolare, analiticamente specificati per iscritto nell’atto di designazione, ed in particolare provvede:

- alla predisposizione del Registro dei trattamenti;
- 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;
- ad individuare, contrattualizzare e nominare i responsabili di trattamento esterni, nel rispetto delle procedure di cui alla normativa europea;
- a definire le informative per gli interessati che dovranno essere realizzate ed apposte in calce alla modulistica ovvero ai servizi on line ovvero affisse nei luoghi di ricevimento del pubblico;
- ad interloquire e collaborare con il Responsabile Protezione Dati ed ad attuare prescrizioni e raccomandazioni, ove possibili, emerse in sede di audit interni;
- a predisporre, qualora necessario in base alle caratteristiche e grado di rischio del trattamento dei dati, in accordo con il Responsabile Protezione Dati, un calendario di audit da svolgere congiuntamente, nei confronti dei responsabili esterni nominati, anche a campione ovvero a rotazione;
- a svolgere, per la parte di competenza, l’analisi d’impatto nei casi ove essa è obbligatoria o comunque significativa in ordine alla corretta gestione dei trattamenti, anche dopo avere consultato il Responsabile Protezione Dati;

- a svolgere l'attività preliminare a seguito di ipotesi di perdita di dati (data breach,) di cui viene a conoscenza ed inoltrare la notifica all'Autorità Garante, sentito, ove il caso, anche il Responsabile Protezione Dati; di dette violazioni dovrà darsi conto in un apposito "registro delle violazioni";

Art. 6 **Responsabile esterno**

1. Il Designato può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di Responsabili esterni del trattamento, 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.

Gli atti che disciplinano il rapporto tra il Designato ed il Responsabile esterno del trattamento devono in particolare contenere quanto previsto dalla normativa comunitaria, a cui si rimanda integralmente.

2. Con l'atto di nomina, il responsabile esterno può essere autorizzato, in via generica o specifica, a nominare sub-responsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Designato ed il Responsabile esterno primario; le operazioni di trattamento possono essere effettuate solo da incaricati autorizzati che operano sotto la diretta autorità del Responsabile esterno attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile esterno risponde, anche dinanzi al/la Designato/a, 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.

Art. 7 **Responsabile Protezione Dati**

1. Il Responsabile Protezione Dati è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed ai designati nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il Responsabile Protezione Dati può indicare al Titolare e/o ai Designati 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 RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Designato. 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 del Designato;

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

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Designato, in particolare, si consulta con il Responsabile Protezione Dati in merito a condurre o meno la valutazione; quale metodologia adottare nel condurla; condurre la valutazione con le risorse interne ovvero esternalizzandola; quali salvaguardie

applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la valutazione sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con l'Autorità Garante e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva prevista dalla normativa europea, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del Responsabile Protezione Dati è comunicato dal Titolare o dal Designato all'Autorità Garante;

f) svolgere altresì i compiti di Responsabile Protezione Dati con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

2. Il Titolare ed il Designato al trattamento assicurano che il Responsabile Protezione Dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e, in particolare, 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 Responsabile Protezione Dati deve essere consultato tempestivamente qualora si verifichi una violazione dei dati (o un altro incidente).

3. Il Titolare fornisce al Responsabile Protezione Dati le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

4. Il Responsabile Protezione Dati opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti e non può essere rimosso o penalizzato dal Titolare e dai Designati del trattamento in ragione dell'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il Responsabile Protezione Dati riferisce direttamente al Titolare o al Designato del trattamento.

Art. 8 Sicurezza del trattamento

1. ARAL Azienda Rifiuti Alessandrina S.p.A. mette in atto misure tecniche ed organizzative idonee a 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 dalla Società:

- 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 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. ARAL Azienda Rifiuti Alessandrina S.p.A si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare e del Responsabile Protezione Dati sono pubblicati sul sito istituzionale della Società, sezione Amministrazione trasparente.

Art. 9

Registro unico delle attività di trattamento

1. Il Registro Unico delle attività di trattamento svolte dal Titolare, tenuto in forma telematica o cartacea, deve contenere almeno le seguenti informazioni:

- a) il nome ed i dati di contatto del Titolare e del RPD;
- b) attività e loro descrizione
- c) le finalità del trattamento;
- d) base giuridica
- e) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- f) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- g) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- h) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- i) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 8.

Art. 10

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 della normativa europea, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La Valutazione 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 valutazione si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità Garante ai sensi del RGDP.

Art. 11
Violazione dei dati personali (“data breach”)

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

2. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

3. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi;
- comportare rischi imminenti e con un'elevata probabilità di accadimento;

4. La notifica deve avere il contenuto minimo previsto dal RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure previste.

5. 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 dall'Autorità Garante al fine di verificare il rispetto delle disposizioni del RGPD.

Art. 12

Particolari categorie di dati

1. Le “particolari categorie di dati” così come definite dal RGPD sono trattate previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi mentre le operazioni di interconnessione, raffronto, comunicazione e diffusione individuate nel presente Regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi e compiti di volta in volta indicati, per il perseguimento delle rilevanti finalità di interesse pubblico specificate e nel rispetto dei limiti stabiliti dalle legge e dai regolamenti.

Art. 13

Videosorveglianza

1. Il presente art. disciplina il trattamento dei dati personali (immagini) acquisiti mediante il sistema di videosorveglianza operativo presso il complesso IPPC “impianto di tmb” sito in Comune di Castelceriolo e presso il complesso IPPC “discarica per rifiuti non pericolosi” sita in Comune di Solero.

2. il trattamento previsto persegue l’interesse legittimo di assicurare, da parte ARAL Azienda Rifiuti Alessandrina S.p.A. la temporanea conservazione di informazioni rilevanti in merito a interventi di emergenza o a interventi su eventi quali incidenti in impianto o intrusioni/accessi non autorizzati solo qualora strettamente necessario, alla ricostruzione della diverse fasi di gestione operativa dell’evento o all’acquisizione di elementi utili a successive indagini da parte dell’Autorità Giudiziaria o delle dell’Autorità di Pubblica Sicurezza, altre che all’acquisizione di prove utili alla predisposizione di denunce/notizie di reato nei casi, pur del tutto particolari, di sottrazione o danneggiamento di beni aziendali.

3. Per tutto quanto non disciplinato nel presente Regolamento, si rinvia a quanto disposto dal Provvedimento dell’Autorità Garante per la protezione dei dati personali in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010)

4. La tipologia di trattamento dei dati personali (acquisizione e conservazione del flusso video) non ricade nelle ipotesi di verifica preliminare (“trattamento che presenta rischi specifici”) del disciplinate dal D.lgs. 196/2003 e ss.mm.ii, (valutazione di impatto ai sensi dell’art. 35 del RGPD), in quanto non presenta potenzialmente rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell’interessato, in relazione alla natura dei dati o alle modalità e finalità del trattamento, o agli effetti che può determinare.

5. Il sistema di videosorveglianza attivato presso il Complesso IPPC “impianto di tmb” sito in Comune di Castelceriolo e presso il complesso IPPC “discarica per rifiuti non pericolosi” sita in Comune di Solero ed il conseguente trattamento di dati personali – che richiede l’ineludibile necessità a posteriori di identificare o rendere potenzialmente identificabili i soggetti eventualmente ricadenti nel raggio di operatività dei sistemi di ripresa - rispetta i principi di necessità e proporzionalità stabiliti dell’Autorità Garante per la protezione dei dati personali in quanto:

- garantisce l’acquisizione di informazioni utili alla ricostruzione di un evento a cui è seguito un intervento, una risposta o, comunque, una “gestione” dell’allarme da con grado di dettaglio maggiore rispetto alle normali annotazioni o rapporti di servizio, anche nel caso in cui non si dovesse verificare un intervento esterno;

- garantisce un necessario presidio di sicurezza per gli operatori aziendali rispetto alle modalità di gestione degli interventi di emergenza e rispetto all'individuazione tempestiva di eventuali anomalie o pericoli in impianto, oltre che di accessi non autorizzati o fraudolenti;
- costituisce una efficace fonte di prova funzionalmente all'accertamento dei reati su autonoma iniziativa, alle attività di indagine disposte dall'Autorità Giudiziaria;
- il flusso video acquisito (in ossequio al principio di proporzionalità) è conservato per un periodo limitato (48 h) ed è accessibile unicamente in caso di denuncia di un fatto penalmente rilevante o di un fatto significativo, anche ai fini della tutela giudiziaria civile o per la definizione di migliori o diverse misure di sicurezza, oltre che mantenere la funzionalità "live".

6. Il sistema di videosorveglianza attivato presso il Complesso IPPC "impianto di tmb" sito in Comune di Castelceriolo e presso il complesso IPPC "discarica per rifiuti non pericolosi" sita in Comune di Solero è protetto con idonee misure di sicurezza, tali da ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini. Sono adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa, e in particolare: in presenza di differenti competenze specificatamente attribuite ai singoli operatori sono configurati diversi livelli di visibilità e trattamento delle immagini ed i soggetti, designati o incaricati sono in possesso di credenziali di autenticazione che permettono di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza, ed è limitata la possibilità, per i soggetti abilitati a visionare non solo in sincronia con la ripresa ma anche in tempo differito le immagini registrate di effettuare sulle medesime operazioni di cancellazione o duplicazione. Il sistema è predisposto per la cancellazione (in "sovrascrittura") in forma automatica, delle registrazioni, allo scadere del termine previsto. In caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si rende indispensabile per effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini. I sistemi di ripresa connessi a reti informatiche e, gli apparati medesimi sono protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale. I dati personali oggetto di trattamento sono costituiti da un flusso video che viene archiviato tramite dvr/nvr, che può essere visionato sia in sincronia con la ripresa che in tempo differito, oltre che importato su ulteriori supporti.

I dati personali acquisiti sono accessibili solo da parte di soggetti appositamente designati e incaricati, con l'osservanza di un sistema di autenticazione basato su credenziali.

7. Ai sensi dell'art. 4, comma 2, L. 300/1970 e ss.mm.ii (Statuto dei lavoratori) "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. (...) In mancanza di accordo, gli impianti e gli strumenti (...) possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro (...)". Il sistema di videosorveglianza che sarà attivato presso il Complesso IPPC "impianto di tmb" sito in Comune di Castelceriolo e presso il complesso IPPC "discarica per rifiuti non pericolosi" sita in Comune di Solero non verrà impiegato per effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa. Non è consentito, da parte di ARAL Azienda Rifiuti Alessandrina S.p.A. un monitoraggio sistematico del flusso video prodotto anche per soli fini statistici o per la rilevazione della posizione o dell'attività svolta dai dipendenti e, in termini

omnicomprensivi, per qualunque forma di controllo a distanza dell'attività dei lavoratori sulla falsariga di quanto rilevato nel provvedimento dell'Autorità Garante per la protezione dei dati personali del 01/08/2012 (doc. web 1923325).

Art. 14

Cessazione del trattamento dei dati

1. In caso di cessazione di un trattamento, per qualsiasi causa, i dati personali acquisiti sono:

- distrutti;
- ceduti ad altro Titolare purché destinati ad un trattamento lecito e conforme agli scopi per i quali i dati sono raccolti;
- conservati per fini esclusivamente istituzionali.

Art. 15

Comunicazione

1. La comunicazione dei dati personali da parte di ARAL Azienda Rifiuti Alessandrina S.p.A. a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è necessaria per lo svolgimento delle funzioni istituzionali e può essere iniziata se è decorso il termine di 45 giorni dalla comunicazione della richiesta all'Autorità Garante ai sensi dell'art. 39, comma 2, del Codice in materia di protezione dei dati personali approvato con D.Lgs 196/2003.

2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte di incaricati e preposti autorizzate per iscritto a compiere le operazioni del trattamento dal Responsabile.

3. E' fatta salva la comunicazione o diffusione di dati richiesti, in conformità disposizioni normative vigenti, da forze di polizia, dall'Autorità Giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art. 16

Rinvio

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