DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)

Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" cosi come modificato dal Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)"

INDICE

1. INTRODUZIONE

Il presente documento costituisce il Documento Programmatico sulla Sicurezza (DPS) dei dati personali che vengono trattati nell'ambito delle attività svolte dalla società C.I.R.A. S.r.l., che attesta e dimostra, insieme agli altri documenti del "dossier privacy", il corretto adempimento di tutti i requisiti previsti dalla normativa vigente in materia di privacy, ai sensi del Regolamento Europeo 2016/679 del 27 Aprile 2016 - Regolamento generale sulla protezione dei dati (di seguito RGPD) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE e ai sensi del D.Lgs. 196/2003 (di seguito codice privacy) cosi come modificato dal D.Lgs. 101/2018.

ORGANIZZAZIONE	C.I.R.A. S.r.l.
SEDE LEGALE ED OPERATIVA	Loc. Piano 6/A – 17058 Dego (SV)
C.F.	92054820094
P.IVA	01221980095
TEL.	019.5778013
PEC	consorziocirasu@pcert.postecert.it
SITO INTERNET	www.ciraservizioidrico.it
CODICE ATECO	36 (Depurazione acque)
NUMERO REA	SV – 128026

Tabella n.1: Anagrafica aziendale

L'obiettivo del presente documento è quello di definire le figure responsabili del trattamento e le relative responsabilità e di stabilire criteri e procedure per il contenimento dei rischi cui è sottoposta le gestione dei dati personali.
Il trattamento di tutti i dati personali da parte dell'organizzazione viene effettuato nel rispetto dei principi definiti all'art.5 del suddetto RGPD, ovvero:

- Liceità (rispetto delle norme), correttezza (rispetto delle reciproche esigenze dell'interessato e del titolare) e trasparenza (verso l'interessato affinché possa legittimamente fondare il proprio consenso)

- Limitazione delle finalità (che devono essere determinate, esplicite e legittime)
- Minimizzazione dei dati raccolti (che devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati)
- Esattezza (i dati raccolti devono essere esatti e, se necessario, aggiornati)
- Limitazione della conservazione (i dati devono essere conservati in una forma che consente l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità o per il tempo previsto per legge)
- Integrità e riservatezza (i dati devono essere trattati in maniera da garantire adeguata sicurezza e protezione)
- Responsabilizzazione del Titolare (rispettare i principi e comprovarlo).

2. TERMINI E DEFINIZIONI

Ai fini del presente documento e dei suoi allegati, si assumono le definizioni indicate all'art.4 del RGPD e dal Decreto nazionale di adeguamento al RGPD:

- "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, 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;
- "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;
- "limitazione di trattamento": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- "profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento

professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- “pseudonimizzazione”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- “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;
- “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;
- “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;
- “destinatario”: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento
- “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;
- “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;

- “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;
- “dati genetici”: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- “dati biometrici”: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- “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;
- “stabilimento principale”:

  -per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

  -con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
- “rappresentante”: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

- “impresa”: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- “gruppo imprenditoriale”: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- “norme vincolanti d'impresa”: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- “autorità di controllo”: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (Garante per la protezione dei dati);
- “autorità di controllo interessata”: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

  -il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

  -gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

  -un reclamo è stato proposto a tale autorità di controllo;
- “trattamento transfrontaliero”:

  -trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

  -trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- “obiezione pertinente e motivata”: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal

progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

- "servizio della società dell'informazione": il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- "organizzazione internazionale": un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati;
- "comunicazione": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "videosorveglianza": installazione di impianti audiovisivi - sistemi di rilevazione e, in generale, di utilizzo di immagini (raccolta, registrazione, conservazione, visione);
- "strumento di lavoro":
  - (Ispettorato del lavoro – Circolare n.2 del 07/11/16) gli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa e che per tale finalità sono stati messi a sua disposizione;
  - (Garante della Privacy) i dispositivi utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa;
  - (Provvedimento del Garante "Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro – 13 luglio 2016"): per esempio il servizio di posta elettronica offerto ai dipendenti mediante attribuzione di un account personale, e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore.

3. COMPITI E RESPONSABILITA'

3.1 Titolare del trattamento

Il titolare del trattamento (*Controller*) è definito dal RGPD come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che […] determina le finalità e i mezzi del trattamento di dati personali" ed è pertanto la società C.I.R.A. S.r.l.

Il titolare del trattamento dei dati personali ha le seguenti responsabilità:

- Mettere in atto, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, misure tecniche e organizzative adeguate per garantire, e poter dimostrare, di effettuare il trattamento in modo conforme al RGPD (artt. 24-25) e un livello di sicurezza adeguato al rischio (art. 32);
- Aggiornare e riesaminare le misure adottate quando necessario;
- Rispettare e poter comprovare che il trattamento dei dati è effettuato nel rispetto dei principi enunciati all'art. 5 del RGPD e al paragrafo 1 del presente documento;
- Individuare le persone autorizzate all'interno della sua struttura al trattamento dei dati per le specifiche finalità e formare il personale;
- Qualora il trattamento sia basato sul consenso (art. 6), deve poter dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei suoi dati personali (art. 7), anche esplicito se trattasi di dati particolari (art.9);
- Adottare misure adeguate per fornire all'interessato tutte le informazioni previste dagli artt. 13 e 14 (informative);
- Garantire agli interessati i diritti di cui godono di cui agli artt. da 15 a 22 del RGPD e la comunicazione in caso di violazione dei dati che sia suscettibile di presentare un rischio elevato per i loro diritti e le loro libertà (art. 34);
- Stipulare un contratto di fornitura o designare uno o più responsabili del trattamento, come meglio definito nel successivo paragrafo, specificando la materia disciplinata, la durata la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati e le responsabilità/compiti del responsabile;
- Tenere in forma scritta un registro delle attività di trattamento svolte sotto la sua responsabilità e, su richiesta, metterlo a disposizione del Garante (art.30 – par. 1 e 3 e 4);

- Cooperare, su richiesta, con il Garante della protezione dei dati nell'esecuzione dei suoi compiti (art. 31);
- In caso di violazioni dei dati (*data breach*), queste devono essere documentate in apposito registro e, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati, notificate al Garante della protezione dei dati senza ingiustificato ritardo e possibilmente entro 72 h da quando ne è venuto a conoscenza (art. 33);
- Effettuare, prima di procedere al trattamento e comunque in caso di variazioni, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, consultandosi, qualora ne sia designato uno, con il responsabile della protezione dei dati (art.35);
- Designare, se del caso, un Responsabile della protezione dei dati (RPD) valutandone le qualità professionali, definendone ruoli e responsabilità e pubblicandone i dati di contatto e comunicandoli al Garante (art. 37).

Qualora il titolare del trattamento sia nominato formalmente da un soggetto terzo come Responsabile dei trattamenti effettuati per suo conto, il titolare provvede, se del caso, a redigere e conservare in forma scritta, anche su supporto elettronico, un registro dei trattamenti ai sensi dell'art. 30, par. 2.

3.2 Responsabile del trattamento

Nei casi in cui il trattamento dei dati personali debba essere effettuato per conto del titolare e i dati debbano essere affidati a soggetti esterni alla struttura del titolare, in virtù di uno o più accordi stipulati tra le parti (contratto o altro atto giuridico) per la fornitura di servizi, si adottano i seguenti criteri, atti a garantire che i soggetti destinatari adottino misure tecniche e organizzative adeguate in modo che il trattamento da loro operato soddisfi i requisiti del RGPD e garantisca la tutela dei diritti degli interessati.

Il soggetto che effettua trattamento di dati personali per conto del titolare del trattamento, viene nominato formalmente dal Titolare mediante apposita lettera scritta quale responsabile del trattamento (*Processor*) dei dati personali ai sensi dell'art. 28 del RGPD.

Nella nomina del responsabile del trattamento sono specificati i compiti e le responsabilità attribuite, tra cui:

- Tenere in forma scritta, anche su supporto elettronico, un registro di tutte le categorie di attività relative al trattamento svolto per conto del titolare del trattamento e, su richiesta, metterlo a disposizione del Garante (art.30 – par. 2 e 3 e 4);
- Cooperare, su richiesta, con il Garante della protezione dei dati nell'esecuzione dei suoi compiti (art. 31);
- Mettere in atto, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, misure tecniche e organizzative adeguate per garantire, e poter dimostrare, un livello di sicurezza adeguato al rischio (art. 32);
- Informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione di dati personali (art. 33 – par. 2);
- Designare, se del caso, un Responsabile della protezione dei dati (RPD) valutandone le qualità professionali, definendone ruoli e responsabilità e pubblicandone i dati di contatto e comunicandoli al Garante (art. 37).

Il titolare ha nominato formalmente tutti i soggetti esterni con cui ha stipulato accordi per la fornitura di servizi, e che, in esecuzione degli accordi, risultano come destinatari ed effettuano trattamenti di dati per conto del titolare.
Tutte le nomine sono ordinatamente raccolte e conservate presso il titolare.

3.3 Responsabile della protezione dei dati

Ai sensi dell'art. 37 del RGPD, se:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico,

- le attività principali del titolare consistono in trattamenti che richiedono il monitoraggio sistematico e regolare degli interessati su larga scala, oppure

- le attività principali del titolare consistono nel trattamento su larga scala di categorie particolari di dati personali (dati sensibili di cui all'art. 9 par. 1) o di dati relativi a condanne penali e reati (art.10),

il titolare del trattamento deve designare un Responsabile della protezione dei dati – RPD (*Data Protection Officer*) valutandone le qualità professionali, la conoscenza specialistica in materia di privacy e della normativa applicabile e le capacità di assolvere ai compiti attribuiti e previsti.

Inoltre, i dati di contatto del RPD devono essere resi pubblici e noti agli interessati e comunicati al Garante.
Il RPD deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e avere a disposizione tutte le risorse necessarie per assolvere ai suoi compiti.

Tenuto conto, col supporto delle Linee guida sui Responsabili della protezione dei dati (WP 243) del Gruppo di lavoro istituito ex art. 29 della Dir. 95/46/CE, che:

- lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri (art. 6, par. 1, lettera e) si potrebbe anche assimilare al caso di autorità pubbliche e potrebbe ricorrere l'ulteriore tutela offerta dalla nomina di un RPD, ma che comunque non sussiste l'obbligo di designazione; C.I.R.A. S.r.l. svolge servizio di fornitura di acqua potabile e depurazione in base ad una convenzione DCP n.60/2016 con la Provincia di Savona in qualità di Gestore del Servizio Idrico Integrato.
- le "attività principali" di un titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria" e si possono quindi intendere come le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento. Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte. D'altro canto, ci sono funzioni di supporto necessarie ai fini dell'attività principale, ma pur essendo necessarie o essenziali sono considerate accessorie e non vengono annoverate fra le attività principali;
- "trattamenti su larga scala" sono quelli che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato;
- non si svolgono attività che possono configurare un monitoraggio regolare e sistematico di interessati su larga scala;
- il trattamento di dati personali è sostanzialmente connesso alla gestione corrente dei rapporti con fornitori, clienti/utenti e personale,

il titolare ha preferito designare volontariamente un Responsabile della protezione dei dati (RPD) ai sensi dell'art. 37 del RGPD, in particolare con riferimento al primo punto esposto (soggetto privato che esercita funzioni pubbliche).

Pertanto rientrando, come raccomandato, nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD, ha provveduto a nominarlo formalmente per iscritto (Atto di designazione del Responsabile della Protezione dei Dati personali del 20/08/2019). Il nominativo e i dati di contatto del RPD sono stati comunicati all'Autorità Garante (Prot. 0011009/2019 del 27/09/2019) e pubblicati sul sito internet.

Nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD il Responsabile è incaricato di svolgere, in piena autonomia e indipendenza, almeno i seguenti compiti e funzioni:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
- cooperare con il Garante per la protezione dei dati personali;
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

4. TRATTAMENTO DI DATI PERSONALI

Il «trattamento» copre una vasta gamma di operazioni eseguite sui dati personali, incluse quelle con mezzi manuali o automatizzati. Comprende 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 di dati personali.

Il trattamento dei dati personali avviene presso la sede legale ed operativa dell'organizzazione in Località Piano 6/A a Dego (SV).

Tutti gli interessati sono preventivamente informati per iscritto dal titolare circa i trattamenti effettuati che li riguardano, le specifiche finalità e i diritti di cui godono. Le suddette informative controfirmate per accettazione e consenso ai trattamenti sono conservate presso il titolare.

Il trattamento effettuato è legittimato ai sensi dell'art.6 del RGPD dalle seguenti condizioni:

- l'interessato ha espresso libero e inequivocabile consenso, controfirmando l'informativa scritta che gli è stata consegnata,
- è necessario all'esecuzione di un contratto di cui l'interessato è parte,
- è necessario per adempiere ad un obbligo legale al quale è soggetto il Titolare,
- è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare (Gestore del Servizio Idrico Integrato: Convenzione DCP n.60/2016 con la Provincia di Savona).

Inoltre, C.I.R.A. S.r.l. effettua il trattamento di categorie particolari di dati personali (es. relativi alla salute e appartenenza sindacale) ai sensi dell'art. 9 del RGPD definiti come "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" relativamente al proprio personale e ad alcune categorie di utenti (non disalimentabili) in base alle disposizioni di legge per assolvere gli obblighi ed esercitare i diritti specifici del titolare e degli interessati in materia di diritto del lavoro e per finalità di medicina del lavoro. Anche in questi casi, viene comunque richiesto esplicito consenso scritto agli interessati per le specifiche finalità di trattamento tramite l'informativa.

Inoltre viene effettuato trattamento di dati giudiziari in base all'art.80 del D.Lgs. 50/2016 - Codice Appalti.

Le finalità dei trattamenti e le rispettive basi giuridiche, oltre alle altre informazioni utili, sono riepilogate nel registro delle attività dei trattamenti svolti sotto la propria responsabilità, redatto in forma scritta su supporto elettronico e conservato ai sensi dell'art. 30 par. 1 del RGPD dal titolare.

Tutti i dati possono essere conservati su supporto cartaceo o informatico.

Il trattamento dei dati e l'accesso ad essi viene effettuato solo ed esclusivamente da soggetti interni alla struttura del titolare autorizzati alle specifiche finalità di trattamento e che hanno ricevuto per ciò un formale incarico, conservato presso il titolare, mediante designazione per iscritto, in accordo ai comma 1 e 2 dell'art. 2-quaterdecies del codice privacy.

Tutte le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare sono preventivamente informate dei loro doveri, in termini di riservatezza sui dati trattati e di misure di sicurezza da adottare. Il personale autorizzato è altresì formato per il trattamento conforme dei dati e, più in generale, in merito alla protezione delle persone fisiche con riguardo ai loro dati personali in conformità al RGPD.

Nell'ambito della presente revisione, sono state verificate le condizioni per la definizione dei profili di autorizzazione e degli ambiti di trattamento consentiti per ciascun incaricato.

Le lettere di incarico resteranno valide fintanto che resteranno confermate le finalità di trattamento di ogni incaricato e non verranno riemesse fino all'insorgenza di eventuali cambiamenti o modifiche ai trattamenti o agli incarichi. Si procederà, pertanto, a verificare periodicamente la definizione dei trattamenti che ciascun incaricato è autorizzato ad esercitare, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

Il trattamento dei dati può essere anche affidato a soggetti esterni alla struttura del titolare, che esercitano in virtù di un contratto o altro atto giuridico un servizio per conto del titolare. In questi casi, tali soggetti esterni sono opportunamente nominati come Responsabili del trattamento dei dati come meglio specificato nel paragrafo dedicato.

Il Garante per la protezione dei dati personali, ai sensi dell'art. 21 del D.Lgs. n.101/2018, ha individuato con Provvedimento n. 146 del 05/06/19 quelle prescrizioni contenute nelle Autorizzazioni generali al trattamento dei dati adottate nel 2016 ancora compatibili con il nuovo Regolamento europeo e con la recente riforma del Codice della privacy.

In particolare, il Garante ha individuato cinque autorizzazioni che contengono specifiche prescrizioni compatibili con il nuovo assetto normativo:

- Autorizzazione generale n. 1/2016 al trattamento di categorie particolari di dati nei rapporti di lavoro;
- Autorizzazione generale n. 3/2016 al trattamento di categorie particolari di dati da parte degli organismi di tipo associativo e delle fondazioni;
- Autorizzazione generale n. 6/2016 al trattamento di categorie particolari di dati da parte degli investigatori privati;
- Autorizzazione generale n. 8/2016 al trattamento dei dati genetici;
- Autorizzazione generale n. 9/2016 al trattamento dei dati personali effettuato per scopi di ricerca scientifica.

Quattro autorizzazioni hanno invece cessato completamente i loro effetti, in particolare: Autorizzazione generale n. 2/2016 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale; Autorizzazione generale n. 4/2016 al trattamento dei dati sensibili da parte dei liberi professionisti; Autorizzazione generale n. 5/2016 al trattamento dei dati sensibili da parte di diverse categorie di titolari; Autorizzazione generale n. 7/2016 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

Il titolare ritiene applicabile l'autorizzazione generale n. 1/2016 e ne prende in carico le prescrizioni.

VIDEOSORVEGLIANZA:

In riferimento al Provvedimento in materia di videosorveglianza - 8 aprile 2010 emanato dal Garante per la protezione dei dati personali (p.to 3.2.3 Notificazione), C.I.R.A. S.r.l. non è tenuta alla notifica al Garante circa i trattamenti di dati relativi all'impianto di videosorveglianza in quanto l'adempimento relativo alla notificazione è stato definitivamente eliminato (art. 22 – c. 8 del D.Lgs. 10 agosto 2018 n. 101).

In particolare, il sistema di videosorveglianza è installato per esigenze di sicurezza, tutela del patrimonio aziendale ed organizzative-produttive, nell'osservanza delle garanzie previste in materia di lavoro (art.4 della Legge n. 300/1970 – Statuto dei lavoratori), come meglio specificato nel modulo di istanza di autorizzazione all'installazione di impianti audiovisivi presentato all'Ispettorato Territoriale del Lavoro di Savona insieme alla relativa Relazione tecnica.

L'attività di raccolta, rilevazione, registrazione, conservazione e, in generale, di utilizzo delle immagini mediante telecamere non viene dunque effettuata 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, e risulta essere condotta in conformità alle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video – Versione 2.0 adottate il 29 gennaio 2020 dall'European Data Protection Board – EDPB e al Provvedimento autorizzativo dell'Ispettorato Territoriale del Lavoro di Savona del 12/07/2022 ai sensi dell'art. 4, comma 2 della Legge n.300/1970, cui si rimanda per i dettagli.

Il trattamento è effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando la ripresa di luoghi circostanti e di particolari che non risultino rilevanti.

I dati trattati sono protetti con idonee misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito o non conforme.

Sono designate per iscritto le persone fisiche incaricate del trattamento specifico, autorizzate sia all'accesso dei locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e visionare le immagini.

La conservazione delle immagini registrate è limitata alle 24 ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura o specifica richiesta investigativa delle autorità. Trascorso il periodo massimo di conservazione, le immagini registrate vengono automaticamente cancellate. È vietata l'acquisizione/registrazione audio.

Il sistema di videosorveglianza non è direttamente collegato con le forze di polizia. I cartelli con apposite informative sono collocati prima del raggio di azione delle telecamere e hanno un formato ed un posizionamento chiaramente visibile in ogni condizione di illuminazione ambientale.

Ogni specifica tecnica relativa all'impianto installato, nonché il posizionamento delle telecamere presso il sito, sono documentati nella Relazione tecnica allegata al Provvedimento autorizzativo.

COOKIE:

Ai sensi del Provvedimento del Garante per la protezione dei dati personali n. 231 del 10 Giugno 2021 – Linee guida cookie e altri strumenti di tracciamento – e del suo Allegato n.1, C.I.R.A. S.r.l. ha provveduto a pubblicare opportuna informativa nella home page del sito internet. L'informativa è conforme a quanto prescritto dal suddetto Provvedimento.

In caso di cookie con funzione non tecnica/di profilazione, per richiedere il consenso all'utilizzo di questi cookie agli utenti del sito, è previsto un banner a comparsa immediata e di adeguate dimensioni che contiene:

- indicazione che il sito utilizza cookie tecnici e, previo consenso dell'utente, cookie di profilazione, con le relative finalità (informativa breve);
- link alla Privacy Policy contenente l'informativa completa;
- l'avvertenza che la chiusura del banner comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookie diversi da quelli tecnici.

Il consenso può essere prestato dall'utente tramite banner secondo quanto prescritto dal suddetto Provvedimento.

GEOLOCALIZZAZIONE:

Con riferimento al Provvedimento n.370 del 4 ottobre 2011 in materia di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro emesso dal Garante, l'organizzazione ha ottenuto dall'Ispettorato Territoriale del Lavoro di Savona in data 14/09/2023 l'autorizzazione ai sensi dell'art. 4, comma 2 della Legge n.300/1970 (Prot. 0007926).

C.I.R.A. S.r.l. ha infatti installato sui suoi vettori un sistema GPS integrato per ragioni di sicurezza del lavoro, tutela del patrimonio aziendale ed esigenze organizzative e produttive, come meglio descritto nella relazione tecnica presentata in sede di istanza di autorizzazione. Da tale sistema potrebbe derivare un controllo indiretto degli autisti e pertanto è stata richiesta e ottenuta autorizzazione.

Adottate le garanzie previste dall'art.4, comma 2, legge n.300/1970, il Titolare può lecitamente effettuare il trattamento dei dati personali relativi all'ubicazione dei propri dipendenti anche in assenza del consenso degli interessati, per effetto del Provvedimento del Garante suddetto, che individua un legittimo interesse al trattamento dei dati.

Ogni specifica tecnica relativa all'impianto installato è documentata nella relazione tecnica allegata come parte integrante del Provvedimento autorizzativo.

Sono informati gli interessati, nominato il responsabile esterno e l'incaricato, apposti gli avvisi sui mezzi e rispettati i tempi di conservazione dei dati.

Anche per questo tipo di trattamento di dati, l'adempimento relativo alla notificazione al Garante è stato definitivamente eliminato (art. 22 – c. 8 del D.Lgs. 10 agosto 2018 n. 101).

DIRETTIVA NIS 2:

C.I.R.A. Srl è stata inserita dalla Agenzia per la Cybersicurezza Nazionale nell'elenco dei soggetti NIS (con codice identificativo ITUFDQ7Q) con le Determinazioni del Direttore Generale n. 136417, 136418, 136435 del 12 aprile 2025,

quale soggetto Essenziale in relazione alle tipologie di soggetto di seguito indicate:

1. Acqua potabile: Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni;

2. Acque reflue: Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale;

3. Organizzazione a cui si applica l'articolo 3, comma 10, del decreto NIS per almeno uno dei criteri di cui alle lettere a), b), c) e d) del medesimo comma.

5. CRITERI PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Premettendo che considerati la natura, il contesto, l'oggetto e le finalità del trattamento, il titolare ritiene non possa derivare dai trattamenti eseguiti alcun rischio grave per i diritti e le libertà degli interessati, in accordo all'art. 35 del RGPD, il titolare del trattamento ha ad ogni modo effettuato una valutazione di impatto dei trattamenti previsti. Anche in considerazione dell'Allegato 1 al Provvedimento n. 467 del 11 ottobre 2018 "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati" che individua al n. 5 i "trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti".

Tale valutazione viene riesaminata periodicamente e comunque ogniqualvolta necessario, per verificane la continua validità a fronte di cambiamenti nei trattamenti effettuati.

L'obiettivo è quello di descrivere, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei trattamenti, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, tutte le misure tecniche e organizzative e di gestione del

rischio poste in essere per garantire, e poter dimostrare, la protezione dei dati personali trattati e un livello di sicurezza adeguato al rischio.

In questa fase vi è la redazione di un elenco completo dei rischi: considerando gli eventi potenzialmente dannosi e fonti di rischio per la sicurezza dei dati personali trattati, vengono valutate la probabilità di accadimento, le possibili conseguenze e la loro gravità e definite le misure di sicurezza previste per affrontare e ridurre i rischi e garantire la protezione dei dati personali degli interessati.

Il metodo adottato per gestire e ponderare i rischi consiste nel calcolare un coefficiente di rischio come prodotto tra la probabilità di accadimento di un evento (P), con riguardo alle minacce, alle fonti di rischio e le misure di sicurezza in essere/pianificate, e la gravità del rischio (G) considerando i potenziali impatti e le misure di sicurezza in essere/pianificate:

Coefficiente di rischio = P x G

Dove:

Probabilità (P)

Valore	Livello	Criteri
4	Altamente probabile	Si sono già verificati casi in numero significativo
3	Probabile	È noto solamente qualche episodio
2	Poco probabile	Sono noti solo rari episodi già verificatisi
1	Improbabile	Non sono noti episodi già verificatisi

Gravità delle Conseguenze (G)

Valore	Livello	Criteri
4	Molto Alto	Eventi che possono comportare rischi elevati per i diritti e le libertà degli interessati
3	Alto	Si possono avere problematiche relative ai diritti e le libertà degli interessati
2	Medio	Possono originarsi problematiche per gli interessati
1	Lieve	Non comporta problemi ai diritti e le libertà degli interessati

E:

Coefficiente di rischio:

	Lieve (1)	Medio (2)	Alto (3)	Molto Alto (4)
Improbabile (1)	Basso	Basso	Medio	Medio
Poco probabile (2)	Basso	Medio	Medio	Alto
Probabile (3)	Medio	Medio	Alto	Alto
Altamente probabile (4)	Medio	Alto	Alto	Alto

Con:

1 ≤ Basso ≤ 2

3 ≤ Medio ≤ 6

8 ≤ Alto ≤ 16

Le misure di sicurezza minime di carattere tecnico e organizzativo e di gestione del rischio adottate e descritte nel file della valutazione di impatto e nel registro dei trattamenti si riferiscono alle infrastrutture del titolare e a tutti i sistemi e gli strumenti elettronici/informatici utilizzati per effettuare il trattamento di dati, anche in caso di adozione di soluzioni di smart-working.
Con riferimento all'art. 9 – Allegato C del Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81 Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza, si richiamano di seguito le misure minime da adottare.

Trattamenti con l'ausilio di strumenti elettronici:

- Identificazione degli utenti, gestione delle identità digitali e implementazione di un sistema di autenticazione e autorizzazione degli utenti (profili di accesso/autorizzazioni a creare-modificare-leggere i dati);

- protezione contro il software malevolo mediante l'impiego di software antimalware aggiornato;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici (dispositivo antivirus, applicativi di blocco dell'accesso a programmi o collegamenti non autorizzati);
- custodia di copie di sicurezza;
- ripristino della disponibilità dei dati e dei sistemi.

Misure di sicurezza fisica e documentale:

- L'accesso alle informazioni è consentito sulla base del principio della necessità di conoscere (need to know);
- la documentazione (supporti cartacei e supporti di memoria come i backup) deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate, ovvero in armadi di sicurezza con procedura di tracciamento delle chiavi in uso.

6. TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI

Il trasferimento di dati verso un paese terzo o organizzazione internazionale è ammesso ai sensi dell'art. 45 del RGPD se la Commissione ha deciso che quel paese/organizzazione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazione specifica.
Le decisioni di adeguatezza sono consultabili direttamente sul sito internet del Garante alla seguente pagina: https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero.
I trasferimenti verso un paese terzo «adeguato» sono pertanto assimilati a una trasmissione di dati all'interno dell'UE.
In mancanza di una decisione di adeguatezza, il titolare può trasferire dei dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate (come esemplificate all'art. 46) e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

In mancanza di una decisione di adeguatezza da parte della Commissione (art.45) o di garanzie adeguate (art.46) è ammesso il trasferimento di dati verso un paese terzo o un'organizzazione internazionale solo se si verificano alcune condizioni, tra cui:

- l'interessato ha esplicitamente dato consenso al trasferimento dopo che esso è stato ben informato sui rischi legati a questi trasferimenti;
- il trasferimento è necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento;
- il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare e un'altra persona fisica o giuridica a favore dell'interessato.

La gestione e conservazione dei dati personali avverrà su server, ubicati all'interno dell'Unione Europea, dell'organizzazione e/o di società terze incaricate e debitamente nominate quali responsabili del trattamento specifico.

I dati non sono attualmente oggetto di trasferimento al di fuori dell'Unione Europea. Resta in ogni caso inteso che l'organizzazione, ove si rendesse necessario, avrà facoltà di spostare l'ubicazione dei server all'interno dell'Unione Europea e/o in Paesi Extra UE.

In tal caso l'organizzazione assicura sin d'ora che il trasferimento dei dati Extra UE avverrà in conformità agli artt. 44 e seguenti del Regolamento e alle disposizioni di legge applicabili stipulando, se necessario, accordi che garantiscano un livello di protezione adeguato.

Dego (SV), 19/06/2025

C.I.R.A. S.r.l.