

## **Data Protection Impact Assessment**

# *Canale interno di segnalazione Whistleblowing*

**Gallo-Road S.r.l.**

**Padova, 15/12/2023**

# Indice

Indice.....	2
Premessa.....	3
1. Introduzione.....	3
2. I soggetti coinvolti.....	4
3. Glossario.....	5
Contesto.....	8
1. Panoramica del trattamento.....	8
2. Dati, processi e risorse di supporto .....	9
Principi fondamentali.....	13
1. Proporzionalità e necessità.....	13
2. Misure a tutela dei diritti degli interessati.....	15
Rischi.....	17
1. Misure esistenti o pianificate.....	17
2. Gestione dei rischi per i diritti e le libertà degli interessati .....	19
2.1 Accesso illegittimo (perdita di riservatezza).....	19
2.2 Modifiche indesiderate (perdita di integrità).....	21
2.3 Indisponibilità dei dati (perdita di disponibilità).....	22
2. Validazione.....	<b>Errore. Il segnalibro non è definito.</b>

# Premessa

## 1. Introduzione

- L'art. 35 del REGOLAMENTO introduce la nozione di valutazione di impatto sulla protezione dei dati (in lingua inglese “*Data Protection Impact Assessment*” o, in breve, “*DPIA*”).
- Una DPIA consiste in 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 (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli). La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del REGOLAMENTO, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni (si veda anche l'art. 24). In altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme.
- Prima di procedere al trattamento, il Titolare è tenuto ad effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento (in particolare allorché preveda l'uso di nuove tecnologie).
- L'obbligo di condurre una valutazione dell'impatto vige anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per i quali intervengano variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi.
- Con il Provvedimento n. 467 dell'11 ottobre 2018 Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati il Garante ha adempiuto all'obbligo posto a suo carico dal quarto comma dell'art. 35 del Regolamento, predisponendo un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.
- L'art. 13, comma 6, del D.Lgs. 24/2023 ha espressamente introdotto l'obbligo di realizzare una valutazione di impatto sul trattamento dei dati personali per i soggetti chiamati ad attivare un canale interno di segnalazione, ai sensi dell'art. 4 del medesimo Decreto.

- Nel momento in cui intenda svolgere una DPIA il Titolare del trattamento è tenuto a consultare il Responsabile per la protezione dei dati, ove ne abbia designato uno ai sensi dell'art. 37 del Regolamento.
- La DPIA contiene almeno i seguenti elementi:
  - a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
  - b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
  - c) una valutazione dei rischi per i diritti e le libertà degli interessati; e
  - d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
- Prima di procedere al trattamento, il Titolare è tenuto a consultare il Garante qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

## 2. I soggetti coinvolti

- Al fine di procedere nel processo di DPIA nel pieno rispetto della Normativa e garantendo un elevato grado di trasparenza del processo, si individuano nella seguente tabella i soggetti che offriranno il proprio contributo prendendo parte alla DPIA.

Nome	Direzione/Ufficio	Ruolo nella DPIA
Dott. Giacomo Lorenzin		• Monitoraggio dello svolgimento della DPIA.
Avv. Marella Mazzei		• Gestore della segnalazione

### 3. Glossario

<b>Archivio</b>	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 (art. 4, comma 1, n. 6 del Regolamento).
<b>Autorità di controllo</b> (di seguito anche il “Garante”)	Garante per la Protezione dei Dati Personali, istituito con legge 31 dicembre 1996 n. 675, ed individuato quale Autorità di controllo ai sensi dell’art. 51 del Regolamento dall’art. 2 <i>bis</i> del Codice.
<b>Categorie particolari di dati personali</b> (di seguito indicati anche come “Dati sensibili”)	Dati 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 (art. 9, comma 1 del Regolamento).
<b>Codice Privacy</b>	Decreto Legislativo n. 196 del 30 giugno 2003, “ <i>Codice in materia di protezione dei dati personali</i> ” e s.m.i.
<b>Comitato Europeo (o “EDPB”)</b>	L’organismo dell’Unione Europea istituito ai sensi dell’art. 68 del Regolamento.
<b>Dati comuni o neutri</b>	Dati personali che non appartengono strettamente alla vita intima della persona, ma riguardano elementi quali le generalità, l’indirizzo, la residenza, il luogo di lavoro, ecc.
<b>Dati giudiziari</b>	Dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza (art. 10 del Regolamento).
<b>Dato personale</b>	Qualsiasi informazione riguardante una persona fisica identificata o identificabile (« <b>interessato</b> »); 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 (art. 4, comma 1, n. 1).
<b>Dati relativi alla salute</b>	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. 4, comma 1, n. 15 del Regolamento).

<b>Destinatario</b>	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 (art. 4, comma 1, n. 9) del Regolamento).
<b>Diffusione</b>	Il mettere a conoscenza dei dati personali soggetti indeterminati, anche mediante la semplice messa a disposizione o consultazione.
<b>Direzione</b> (o “Area” o “Ufficio”)	Struttura organizzativa della Società.
<b>Gallo-Road</b>	Gallo-Road S.r.l. Via Pietro Maroncelli, 23, 35129 Padova, CF 00220250286
<b>Interessato</b>	La persona fisica identificata o identificabile cui siano riferibili i dati personali (art. 4, comma 1, n. 1) del Regolamento).
<b>Normativa</b>	Si intende (1) il REGOLAMENTO; (2) il Codice Privacy; (3) ogni legge, provvedimento avente efficacia di legge, regolamento che disciplini la materia del trattamento dei dati personali applicabile; (4) ogni altro Provvedimento emesso dal Garante e/o dal Comitato Europeo.
<b>Parola chiave</b> (o “Password”)	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
<b>Persone autorizzate al trattamento dei dati personali</b> (anche “Incaricati”)	I soggetti – autorizzati ed istruiti - che hanno accesso a dati personali e agiscono sotto l'autorità del Titolare o del Responsabile del trattamento (art. 29 del Regolamento).
<b>Profilo di autorizzazione</b>	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
<b>Registro dei trattamenti</b>	I Registri delle attività di trattamento tenuto dalla Società ai sensi dell'art. 30 del Regolamento.
<b>Regolamento</b> (o “REGOLAMENTO”)	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, “ <i>Regolamento Generale sulla protezione dei dati personali</i> ”.
<b>Responsabile del trattamento</b>	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, comma 1, n. 8, del Regolamento).
<b>Sistema di autorizzazione</b>	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

<b>Società</b>	Gallo-Road S.r.l. Via Pietro Maroncelli, 23, 35129 Padova, CF 00220250286
<b>Titolare del trattamento</b>	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 (art. 4, comma 1, n. 7, del Regolamento).
<b>Trattamento</b>	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” (art. 4, comma 1, n. 2 del Regolamento).
<b>Valutazione d'impatto sulla protezione dei dati</b> (anche “ <i>Data Protection Impact Assessment</i> ” o “DPIA”)	Valutazione preventiva effettuata dal Titolare del trattamento in relazione a tipologie di trattamento che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevedano in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento (art. 35 del Regolamento).
<b>Violazione dei dati personali</b> (anche “Violazione” o “ <i>Data breach</i> ”)	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 (art. 4, comma 1, n. 12 del Regolamento).
<b>WP 29</b>	Il Gruppo di lavoro istituito ai sensi dell’art. 29 della Direttiva 95/46/EC, ora soppresso e sostituito dall’EDPB.

# Contesto

## 1. Panoramica del trattamento

### Individuazione del trattamento oggetto di DPIA

Gallo-Road S.r.l. (di seguito anche “**Gallo-Road**” o la “**Società**”) è una società attiva nel settore delle costruzioni edili. Gallo-Road opera in diversi campi dell’edilizia quali: edilizia residenziale, edilizia pubblica, edilizia industriale, opere idrauliche, infrastrutture stradali, realizzazione di parchi ornamentali pubblici e privati.

La Società, avendo oltre 50 dipendenti, rientra tra i soggetti tenuti ad attivare, a decorrere dal 17.12.2023, un proprio canale interno idoneo a consentire la **gestione delle segnalazioni**, effettuate dai soggetti di cui all’art. 3, comma 3, del Decreto Whistleblowing, di comportamenti illeciti, commissivi od omissivi che costituiscano o possano costituire una violazione ai sensi del Decreto Whistleblowing stesso.

La violazione oggetto della segnalazione può consistere in comportamenti, atti od omissioni che ledono l’interesse pubblico o l’integrità della Società (come, ad es., illeciti amministrativi, contabili, civili o penali o violazioni del Modello Organizzativo)<sup>1</sup>.

Le Società hanno valutato di organizzare il proprio canale interno di segnalazione in modalità cartacea.

Le attività di gestione del canale interno di segnalazione comportano necessariamente la raccolta di informazioni relative, a titolo esemplificativo, all’identità e alla mansione del soggetto che compie la segnalazione (di seguito, il “**Segnalante**”); all’identità, alla mansione e agli ulteriori atteggiamenti e/o comportamenti dei soggetti menzionati nella segnalazione (di seguito, le “**Persone coinvolte**”); nonché ad ogni ulteriore circostanza rilevante ai fini della segnalazione.

<sup>1</sup> Per un elenco delle fattispecie rilevanti ai fini dell’integrazione di una violazione si rimanda alla Procedura Whistleblowing.



	<p>Molte delle informazioni appena menzionate sono qualificabili come <b>dati personali</b> ai sensi della vigente Normativa. Una descrizione più approfondita delle tipologie e della natura dei dati personali raccolti nell'ambito del trattamento in oggetto può essere rinvenuta al successivo paragrafo "<i>Dati, processi e risorse di supporto</i>".</p> <p>La Società intende effettuare la presente valutazione di impatto sulla protezione dei dati (in lingua inglese "<i>Data Protection Impact Assessment</i>" o, in breve, "<b>DPIA</b>"), nel rispetto dell'art. 35 del Regolamento (UE) 2016/679 (il "<b>REGOLAMENTO</b>" o "<b>Regolamento</b>"), con specifico riferimento al trattamento dei dati personali realizzato nell'ambito della gestione del canale di segnalazione interna. In particolare, la sottoposizione a DPIA del trattamento in oggetto risulta necessaria in quanto espressamente prevista dall'art. 13, comma 6, del Decreto Whistleblowing.</p>
<p><b>Individuazione delle responsabilità connesse al trattamento</b></p>	<p>Nell'ambito delle attività di trattamento dei dati personali connesse alla gestione del canale di segnalazione interna agisce, in qualità di titolare del trattamento, Gallo-Road.</p> <p>Ai sensi dell'art. 4, comma 2, del Decreto Whistleblowing, la gestione del canale di segnalazione è affidata ad una persona esterna che, nell'ambito della realizzazione delle attività connesse al canale di segnalazione, è autonoma e specificamente formata (di seguito, il "<b>Gestore</b>").</p> <p>Il Gestore – individuato nella figura dell'Avv. Marella Mazzei – ha ricevuto l'autorizzazione e le istruzioni per il trattamento da parte di tutte le Società, attraverso apposito atto scritto. In particolare, il Gestore, ai sensi dell'art. 29 del REGOLAMENTO e 2-quaterdecies del D.Lgs. 196/2003 (di seguito, il "<b>Codice Privacy</b>"), è autorizzato al trattamento dei dati personali contenuti nelle segnalazioni o raccolti nel corso del processo di gestione delle segnalazioni medesime.</p>

## 2. Dati, processi e risorse di supporto

<p>Numero di potenziali interessati</p>	
---	--

	<p>Il numero di potenziali interessati dal trattamento oggetto di valutazione non può essere stabilito con esattezza.</p> <p>Con ogni probabilità gli interessati coinvolti appartengono al “contesto lavorativo” della persona segnalante, così come definito dall’art. 2, comma 1, lett. i) del Decreto <i>Whistleblowing</i>.</p> <p>Non può escludersi, però, che le persone coinvolte dalla segnalazione e dai fatti ad essa relativi siano esterne rispetto al contesto lavorativo del segnalante e/o che il segnalante stesso non appartenga direttamente ad alcuna delle Società, bensì rientri tra gli ulteriori soggetti di cui all’art. 3, comma 3, del Decreto <i>Whistleblowing</i>.</p>
<p><b>Categorie di interessati</b></p>	<ul style="list-style-type: none"> <li>✓ <b>(Persona) Segnalante</b>, come definito all’art. 2, comma 1, lett. g) del Decreto <i>Whistleblowing</i> ossia “<i>la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell’ambito del proprio contesto lavorativo</i>” e come individuato/i all’art. 3, comma 3, del Decreto <i>Whistleblowing</i>;</li> <li>✓ <b>Persona coinvolta</b>, come definita all’art. 2, comma 1, lett. l) del Decreto <i>Whistleblowing</i> ossia “<i>la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente</i>”;</li> <li>✓ <b>(Eventuale) Facilitatore</b>, come definito all’art. 2, comma 1, lett. g) del Decreto <i>Whistleblowing</i> ossia “<i>una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all’interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata</i>”;</li> <li>✓ <b>Gestore coinvolto nel processo di gestione della segnalazione</b>;</li> </ul> <p>Ogni altro soggetto che possa essere <b>menzionato nella segnalazione e coinvolto</b> nel fatto così come descritto dal Segnalante (ad es., altri dipendenti, eventuali fornitori, gli organi di vigilanza e controllo o ulteriori soggetti terzi).</p>
<p><b>Categorie di dati personali</b></p>	<ul style="list-style-type: none"> <li>✓ <b>Dati comuni</b>: nome e cognome, codice fiscale, dati di contatto o dati inerenti alla mansione esercitata nel contesto lavorativo del Segnalante, dati inseriti nella segnalazione o nella documentazione allegata o raccolti durante il processo di gestione della segnalazione.</li> <li>✓ <b>Eventuali categorie particolari di dati</b>, di cui all’art. 9 del REGOLAMENTO, ove contenuti nella segnalazione o il cui trattamento risulti necessario ai fini della gestione della segnalazione medesima;</li> </ul>

	<p>✓ <b>Eventuali dati relativi a condanne penali e reati</b>, di cui all'art. 10 del REGOLAMENTO, ove contenuti nella segnalazione o il cui trattamento risulti necessario ai fini della gestione della segnalazione medesima.</p>
<p><b>Descrizione funzionale del trattamento</b></p>	<p>Il trattamento dei dati personali avviene ai sensi della Procedura di Whistleblowing adottata dalla Società, che costituisce parte integrante della presente DPIA (di seguito, la “<b>Procedura</b>” o la “<b>Procedura Whistleblowing</b>”).</p> <p>Si tengano in considerazione le seguenti fasi che definiscono il <b>ciclo di vita dei dati</b> soggetti a trattamento:</p> <p>✓ <b>Raccolta:</b> i dati personali forniti in sede di segnalazione vengono raccolti:</p> <p>a) <u>In forma scritta</u>, tramite posta ordinaria, in tripla busta chiusa che rechi all'esterno la dicitura “riservata/personale all'attenzione dell'Avv. Marella Mazzei”, da inviare all'indirizzo: Via Marconi 15, 356122 Padova. La segnalazione deve essere inserita in due buste chiuse: la prima con i dati identificativi del Segnalante unitamente alla fotocopia del suo documento di riconoscimento; la seconda con la descrizione dei fatti da segnalare. Entrambe le buste saranno poi inserite in una terza busta chiusa che rechi all'esterno la dicitura di cui sopra.</p> <p>b) <u>In forma orale</u>, attraverso la linea telefonica dedicata, chiamando il numero 3381181727, a cui ha accesso esclusivamente il Gestore. Su richiesta del Segnalante, il Gestore potrà altresì organizzare un incontro per raccogliere le informazioni in merito alla Segnalazione.</p> <p>✓ <b>La protocollazione della Segnalazione:</b> il Gestore, entro 7 giorni dalla data di ricezione della Segnalazione, deve rilasciare un avviso di ricevimento al Segnalante, tramite i contatti da questo riportati in occasione della Segnalazione. Il Gestore, in linea con le istruzioni ricevute al momento della designazione, è tenuto ad attribuire un numero progressivo di protocollo a ciascuna Segnalazione e a conservarla, assieme alla relativa documentazione, in un archivio fisico chiuso a chiave, a cui solo lui/lei ha accesso. Nel caso in cui la segnalazione sia corredata di documentazione in formato digitale, questa deve essere conservata in archivi protetti da chiavi di accesso, a cui deve poter accedere esclusivamente il Gestore.</p>

- ✓ **La valutazione della Segnalazione:** il Gestore esamina la segnalazione e valuta in via preliminare l'ammissibilità della stessa e la sua fondatezza secondo i criteri stabiliti nella Procedura (sul punto, si veda il par. 3.2 della Procedura Whistleblowing). Qualora il Gestore ritenga la Segnalazione ammissibile e circostanziata con elementi di fatto precisi e concordanti, procede alla fase istruttoria di investigazione avvalendosi, in caso di esigenza, di altra funzione interna competente. In tale caso, il Gestore comunicherà con la funzione coinvolta garantendo la riservatezza e l'anonimato delle Segnalante e delle ulteriori persone coinvolte nella Segnalazione. In particolare, salvo l'espreso consenso del Segnalante, il Gestore non comunicherà ad alcuno i suoi dati personali o ulteriori informazioni da cui si possa evincere la sua identità. Al termine dell'attività di indagine il Gestore, prima di riscontrare il Segnalante, valuta se archiviare la Segnalazione o procedere alla sua trasmissione, secondo quanto previsto dal par. 3.3 della Procedura.
- ✓ **La trasmissione della Segnalazione:** nel caso in cui la Segnalazione risulti ricevibile e fondata, il Gestore procede alla trasmissione secondo le modalità ed ai soggetti indicati al par. 3.4 della Procedura.
- ✓ **Riservatezza e sicurezza:** i dati personali vengono trattati con la massima riservatezza e sicurezza. Vengono adottate misure per proteggere l'accesso non autorizzato, l'uso improprio o la divulgazione dei dati al fine di preservare la privacy del Segnalante e garantire la conformità alle leggi sulla protezione dei dati personali. Il Gestore ha previamente ricevuto dalla Società precise istruzioni di trattamento ed ha sottoscritto appositi accordi di riservatezza. Le misure tecniche di sicurezza adottate saranno descritte nel prosieguo.
- ✓ **Conservazione dei dati:** I dati personali contenuti nella Segnalazione e nella documentazione relativa al processo di gestione della Segnalazione medesima, saranno conservati a cura del Gestore in appositi archivi, fisici o digitali, a cui solo lui/lei ha accesso. In particolare, i dati potranno essere conservati in formato cartaceo in apposito armadio/archivio chiuso a chiave situato presso gli uffici del Gestore. I dati personali verranno conservati per il periodo di tempo necessario al trattamento della Segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. Una volta scaduto il periodo di conservazione, i dati personali verranno eliminati in modo sicuro e irreversibile.

<p><b>Risorse tecniche utilizzate per il trattamento</b></p>	<p>La Società ha deciso di adottare il Canale interno di segnalazione in modalità cartacea. Le segnalazioni ed i successivi contatti con il Gestore, pertanto, possono avvenire tramite posta cartacea o tramite la linea telefonica nell'esclusiva disponibilità del Gestore della segnalazione.</p>
--	---

## Principi fondamentali

### 1. Proporzionalità e necessità

<p><b>Principio di limitazione della finalità</b></p>	<p>Le Società hanno individuato in maniera specifica ed esplicita le <b>finalità</b> del trattamento dei dati personali, ossia <b>l'Adempimento degli obblighi di legge</b> previsti dal Decreto Whistleblowing e la relativa tutela del soggetto Segnalante.</p> <p>Tra gli obblighi introdotti dal Decreto Whistleblowing in questione, rilevano in particolare;</p> <ul style="list-style-type: none"> <li>✓ L'attivazione e la gestione di un proprio canale interno di segnalazione (cfr. art. 4 del Decreto Whistleblowing);</li> <li>✓ La conservazione della documentazione relativa alla segnalazione (art. 14 del Decreto Whistleblowing);</li> <li>✓ La verifica della <b> fondatezza della segnalazione e gestione della medesima </b> in tutte le sue fasi, incluse quelle di accertamento dei fatti oggetto di segnalazione e di adozione di eventuali e conseguenti provvedimenti/azioni (cfr. paragrafo 3.4 della Procedura Whistleblowing).</li> </ul> <p>I dati raccolti mediante il Canale interno di segnalazione o nel corso delle varie fasi di gestione delle Segnalazioni potranno essere trattati unicamente per le finalità di cui sopra, essendo categoricamente escluso ogni loro impiego ulteriore.</p>
---	--

	<p>La Società ha fornito <b>indicazioni precise</b> ai soggetti incaricati in merito alle finalità del trattamento, anche mediante la predisposizione della Procedura Whistleblowing e la sottoscrizione di appositi atti di designazione.</p>
<p><b>Principio di liceità del trattamento</b></p>	<p>La <b>base giuridica</b> che rende lecito il trattamento consiste nella necessità di <u>adempiere ad un obbligo legale</u> al quale è soggetto il titolare del trattamento (art. 6, comma 1, lett. c) del Regolamento).</p> <p>Nell'ambito di un eventuale procedimento disciplinare nei confronti delle Persone coinvolte e negli altri casi previsti dalla normativa e dalla Procedura, le Società, anche ai sensi dell'art. 12 del Decreto Whistleblowing, necessiteranno del consenso del Segnalante a rivelare la sua identità (art. 6, comma 1, lett. a) del Regolamento).</p> <p>Nei limiti in cui sia strettamente necessario al perseguimento delle finalità di cui sopra, la Società potrà trovarsi a trattare anche dati personali appartenenti a categorie particolari di cui all'art. 9 del Regolamento (es. dati relativi alla salute, all'appartenenza sindacale, dati idonei a rivelare origine razziale, opinioni politiche, convinzioni religiose o filosofiche dell'interessato, etc.) o dati relativi a condanne penali e reati di cui all'art. 10 del Regolamento, ove eventualmente contenuti nella segnalazione ed indispensabili perché la Società possa darne seguito. Tale trattamento avverrà in quanto strettamente necessario ad assolvere un obbligo di legge (ai sensi dell'art. 6, comma 1, lett. c), art. 9, comma 2, lett. b) e art. 10 del Regolamento). Tali dati in ogni caso non potranno essere oggetto di rivelazione nell'ambito dell'eventuale procedimento disciplinare.</p> <p>Nel caso di necessità di rivelare a persone diverse dal Gestore l'identità della persona Segnalante, o qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità, si procederà a richiedere al Segnalante medesimo un espresso e specifico consenso, ai sensi dell'art. 12, comma 2 e ss. del D.Lgs. 24/2023 ed art. 6 comma 1, lett. a) del Regolamento.</p> <p>Il consenso sarà facoltativo e potrà essere liberamente revocato in qualsiasi momento secondo le modalità che saranno indicate in sede di richiesta.</p>
<p><b>Principio di minimizzazione dei dati</b></p>	<p>I dati trattati appaiono <b>adeguati, pertinenti e limitati</b> a quanto è necessario in relazione alle finalità di trattamento specificate sopra.</p> <p><b>Nello specifico</b>, ai sensi dell'art. 13, comma 2, del Decreto Whistleblowing ed in linea con la Procedura Whistleblowing, verranno presi in considerazione e saranno oggetto di trattamento ai fini della fase istruttoria</p>

	<p>ed investigazione ad opera del Gestore <b>soltanto</b> i dati e le informazioni forniti dal Segnalante rilevanti per la descrizione del fatto o delle circostanze avvenute in sua presenza e/o di cui questi abbia evidenza documentale.</p> <p>In particolare:</p> <ul style="list-style-type: none"> <li>- il trattamento dei dati del Segnalante si rende necessario al fine di verificare l'attendibilità della Segnalazione e, eventualmente, al fine di dare corso, previo l'ottenimento del consenso del Segnalante stesso, al procedimento disciplinare, anche ai sensi di quanto previsto dall'art. 12 del Decreto Whistleblowing;</li> <li>- il trattamento dei dati delle Persone coinvolte è necessario al fine di consentire alle Società di valutare l'attendibilità e le circostanze della segnalazione.</li> </ul> <p>Come specificato nella Procedura Whistleblowing, tutti i dati <b>manifestamente non utili</b> non devono essere inseriti nella Segnalazione e, se comunque forniti dal Segnalante, saranno immediatamente cancellati.</p>
<p><b>Principio di correttezza dei dati</b></p>	<p>Il Gestore è tenuto a consentire al Segnalante la possibilità di verificare e/o rettificare e/o integrare la propria precedente Segnalazione. Inoltre, il Gestore può, se necessario, richiedere al Segnalante eventuali integrazioni.</p> <p>Resta inteso che, come di seguito specificato, l'esercizio dei diritti di cui agli artt. 15 a 22 del Regolamento potrà essere soggetto a limitazioni (ai sensi dell'art. 2-undecies del Codice Privacy).</p>
<p><b>Principio di limitazione della conservazione</b></p>	<p>In ottemperanza agli articoli 12 e 14 del Decreto Whistleblowing, le Segnalazioni <b>non saranno utilizzate</b> oltre quanto necessario per dare seguito alle stesse e <b>saranno conservate</b>, con la relativa documentazione, non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza previsti dalla normativa.</p>

## 2. Misure a tutela dei diritti degli interessati

<p><b>Informazioni fornite agli interessati</b></p>	
---	--

	<p>Gli Interessati vengono informati in maniera chiara e trasparente circa il trattamento in oggetto, in linea con quanto previsto dagli articoli 13 e 14 del REGOLAMENTO.</p> <p>Tali informazioni vengono fornite agli interessati per mezzo dell'Informativa Whistleblowing pubblicata nel sito web della Società e resa disponibile negli ambienti comuni (quali, ad es., le bacheche aziendali).</p> <p>Nei casi in cui, nell'ambito di un eventuale procedimento disciplinare, il disvelamento dell'identità del Segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare o della Persona coinvolta, il Gestore richiederà al Segnalante un valido ed espresso consenso alla rivelazione della sua identità (art. 6, comma 1, lett. a), del Regolamento). In tale circostanza, verrà consegnata nuovamente al Segnalante l'Informativa Whistleblowing e gli verranno comunicate le modalità con le quali revocare il consenso eventualmente conferito.</p>
<p><b>Diritti di cui agli artt. da 15 a 22 del Regolamento</b></p>	<p>Gli Interessati possono esercitare i diritti riconosciuti dagli artt. da 15 a 22 del REGOLAMENTO nei casi e secondo i limi previsti dal Regolamento contattando il Gestore.</p> <p>Ad ogni modo, la Società potrà limitare l'esercizio dei diritti degli Interessati in ragione di quanto previsto dall'art. 2-undecies del Codice privacy o di altre normative applicabili. Gli interessati, inoltre, sono informati della facoltà di esercitare i diritti in questione per il tramite del Garante per la protezione dei dati personali con le modalità di cui all'art. 160 del Codice Privacy.</p>
<p><b>Rapporti con i responsabili del trattamento</b></p>	<p>Il Gestore è un soggetto esterno alla società Gallo-Road. Per quanto concerne il trattamento di dati personali, il Gestore agisce sotto la diretta autorità del titolare del trattamento e, pertanto, è stato designato ai sensi degli artt. 29 e 2-quaterdecies del Regolamento.</p> <p>Al momento non sono previsti responsabili del trattamento. Nel caso in cui, nell'ambito delle attività di gestione delle Segnalazioni, sia necessario ricorrere ad eventuali consulenti esterni o ulteriori soggetti che agiscono in qualità di responsabili del trattamento, la Società provvederà a nominare tali soggetti ai sensi dell'art. 28 del Regolamento.</p>
<p><b>Garanzie per i trasferimenti internazionali di dati</b></p>	



I dati personali trattati nell'ambito della gestione del Canale interno di segnalazione Whistleblowing non saranno oggetto di trasferimento verso Paese non appartenenti all'Unione Europea.

## Rischi

### 1. Misure esistenti o pianificate

#### Misure di sicurezza tecniche

Le Segnalazioni orali avverranno tramite **un'utenza telefonica appositamente dedicata** a cui il solo Gestore ha accesso.

Il Gestore potrà comunicare con il Segnalante attraverso posta cartacea (raccomandata con ricevuta di ritorno), oppure attraverso gli ulteriori contatti messi a disposizione dal Segnalante. Nel caso in cui le comunicazioni avvengano via mail il Gestore opera con una **casella mail a cui ha esclusivo accesso tramite credenziale personali**.

Nel caso di trattamento di dati tramite supporti informatici, si specifica che tutti i device in dotazione delle Società sono forniti di appositi **programmi antivirus**, i quali vengono periodicamente aggiornati.

## Misure di sicurezza organizzative

**Designazione dei soggetti autorizzati al trattamento ai sensi degli artt. 2-quaterdecies del Codice Privacy e 29 del Regolamento:** il Gestore è stato appositamente designato, con il conferimento di specifico profilo di autorizzazione al trattamento. Nel caso in cui, nell'ambito della gestione delle Segnalazioni, sia necessario comunicare i dati personali ivi contenuti ad altro soggetto interno, secondo le modalità previste dalla Procedura Whistleblowing e dal Decreto Whistleblowing, tale ulteriore soggetto ricevere una specifica designazione a cura del titolare.

**Previsione obblighi di confidenzialità:** i soggetti designati internamente quali autorizzati al trattamento sono sottoposti a obblighi di riservatezza in relazione al trattamento dei dati personali. Questo impegno è esplicitato negli atti di nomina/designazione conferiti dalla Società.

### **Formazione e informazione:**

1. La Società ha programmato iniziative periodiche di sensibilizzazione del personale per divulgare le finalità dell'istituto del "whistleblowing" e la procedura per il suo utilizzo;
2. Il Gestore ha garantito alle Società di possedere l'adeguata professionalità volta ad assicurare che la gestione delle segnalazioni interne sia svolta in conformità alle previsioni normative applicabili.

**Procedura per la gestione delle segnalazioni whistleblowing:** la Società ha adottato la Procedura Whistleblowing che definisce gli adempimenti da porre in essere durante tutte le fasi del processo di gestione delle segnalazioni, anche con riguardo agli aspetti di sicurezza e di trattamento delle informazioni e dei dati personali.

	<p><b>Strumenti di informativa per gli Interessati:</b> gli Interessati sono informati mediante apposita informativa relativa al trattamento dei dati, disponibile sul sito web delle Società e negli ambienti comuni (ad es., nella bacheca aziendale).</p>
	<p><b>Comunicazioni riservate/personali:</b> ai sensi della Procedura Whistleblowing, tutte le comunicazioni per posta cartacea destinate al Gestore devono essere contraddistinte dalla dicitura “riservata/personale” apposta all'esterno della busta.</p>
	<p><b>Tripla busta chiusa:</b> ai sensi della Procedura Whistleblowing, le Segnalazioni devono avvenire in tripla busta chiusa, al fine di tutelare la riservatezza del Segnalante.</p>

## 2. Gestione dei rischi per i diritti e le libertà degli interessati

### 2.1 Accesso illegittimo (perdita di riservatezza)

<p>Quali sono le principali <u>minacce</u> che potrebbero concretizzare il rischio?</p>	<ul style="list-style-type: none"> <li>➤ <b>Errori non intenzionali o negligenze</b></li> <li>➤ <b>Attacchi intenzionali</b></li> <li>➤ <b>Minacce derivanti da fattori industriali</b> (ad es., interruzione di servizi essenziali a garantire la sicurezza delle informazioni)</li> </ul>
<p>Quali sono le <u>fonti</u> del rischio?</p>	<p>Le fonti del rischio sono di natura umana, interna o esterna rispetto alla Società.</p>
<p>Quali potrebbero essere i principali <u>impatti</u> sugli interessati se il rischio si dovesse concretizzare?</p>	<p>I principali impatti sugli interessati potrebbero essere:</p> <ul style="list-style-type: none"> <li>- Perdita di controllo sui propri dati personali;</li> <li>- Furto di identità;</li> </ul>

	- Danno sociale e/o pregiudizio alla reputazione.	
Quali <u>misure</u> fra quelle individuate contribuiscono a mitigare il rischio?	<u>Utenza telefonica dedicata, indirizzo di posta cartacea dedicato del Gestore della Segnalazione</u>	L'adozione di tali misure è finalizzata a minimizzare il rischio che soggetti non espressamente autorizzati al trattamento riescano ad accedere ai dati trattati nell'ambito della gestione del Canale interno di segnalazione Whistleblowing.
	<u>Designazione dei soggetti autorizzati al trattamento; attività di formazione; adozione della Procedura Whistleblowing.</u>	L'adozione di tali misure è finalizzata a regolamentare i processi legati alla gestione del canale interno di segnalazione e a fornire specifiche istruzioni di trattamento ai soggetti coinvolti, nonché a vincolarli agli obblighi di riservatezza.
Come stimereste la <u>gravità</u> del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	<input type="checkbox"/> Trascurabile <input checked="" type="checkbox"/> Limitata <input type="checkbox"/> Importante <input type="checkbox"/> Massimo	<p>Tale stima è stata elaborata alla luce dei seguenti fattori:</p> <ul style="list-style-type: none"> <li>- Trattamento realizzato per un numero limitato di finalità;</li> <li>- Limitato accesso ai dati personali;</li> <li>- Minimizzazione dei dati trattati.</li> </ul>
Come stimereste la <u>probabilità</u> del rischio, specialmente con riguardo alle	<input type="checkbox"/> Trascurabile <input checked="" type="checkbox"/> Limitata <input type="checkbox"/> Importante	

<p>minacce, alle fonti del rischio e alle misure pianificate?</p>	<p><input type="checkbox"/> Massima</p> <p>Le misure organizzative e tecniche di sicurezza adottate dalle Società consentono di stimare la probabilità del rischio derivante dalle fonti di cui sopra come limitata.</p>
---	--

## 2.2 Modifiche indesiderate (perdita di integrità)

<p>Quali sono le principali <u>minacce</u> che potrebbero concretizzare il rischio?</p>	<p>Le principali minacce potrebbero essere:</p> <ul style="list-style-type: none"> <li>- atto doloso;</li> <li>- Errori o comportamenti accidentali.</li> </ul>	
<p>Quali sono le <u>fonti</u> del rischio?</p>	<p>Le fonti del rischio sono di natura:</p> <ul style="list-style-type: none"> <li>- Umana, interna o esterna rispetto alla Società.</li> </ul>	
<p>Quali potrebbero essere i principali <u>impatti</u> sugli interessati se il rischio si dovesse concretizzare?</p>	<p>Perdita del controllo sui dati.</p>	
<p>Quali <u>misure</u> fra quelle individuate contribuiscono a mitigare il rischio?</p>	<p><u>Utenza telefonica dedicata, indirizzo di posta cartacea dedicato del Gestore della Segnalazione.</u></p>	<p>L'adozione di tali misure consente alla Società di limitare il numero di soggetti che hanno accesso ai dati personali.</p>
	<p><u>Designazione dei soggetti autorizzati al trattamento; attività di formazione; adozione della Procedura Whistleblowing.</u></p>	<p>L'adozione di tali misure consente alla Società di istruire in maniera dettagliata i soggetti coinvolti nei trattamenti.</p>
<p>Come stimereste la <u>gravità</u> del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?</p>	<p><input type="checkbox"/> Trascurabile  <input checked="" type="checkbox"/> Limitata  <input type="checkbox"/> Importante</p>	

	<input type="checkbox"/> Massimo Tale stima è stata elaborata alla luce dei seguenti fattori: <ul style="list-style-type: none"> <li>- Presenza di procedure specifiche per l'archiviazione dei dati personali;</li> <li>- Presenza di specifici profili di autorizzazione in merito agli accessi ai dati personali.</li> </ul>
<b>Come stimereste la <u>probabilità</u> del rischio, specialmente con riguardo alle minacce, alle fonti del rischio e alle misure pianificate?</b>	<input type="checkbox"/> Trascurabile <input checked="" type="checkbox"/> Limitata <input type="checkbox"/> Importante <input type="checkbox"/> Massima  Le misure organizzative e tecniche di sicurezza adottate dalle Società consentono di stimare la probabilità del rischio derivante dalle fonti di cui sopra come limitata.

### 2.3 Indisponibilità dei dati (perdita di disponibilità)

<b>Quali sono le principali <u>minacce</u> che potrebbero concretizzare il rischio?</b>	Le principali minacce potrebbero essere: <ul style="list-style-type: none"> <li>- atto doloso;</li> <li>- Errori o comportamenti accidentali.</li> </ul>
<b>Quali sono le <u>fonti</u> del rischio?</b>	Le fonti del rischio sono di natura: <ul style="list-style-type: none"> <li>- Umana, interna o esterna rispetto alla Società;</li> <li>- Altro, quali calamità naturali.</li> </ul>
<b>Quali potrebbero essere i principali <u>impatti</u> sugli interessati se il rischio si dovesse concretizzare?</b>	Perdita del controllo sui dati.

Quali <u>misure</u> fra quelle individuate contribuiscono a mitigare il rischio?	<u>Utenza telefonica dedicata, indirizzo di posta cartacea dedicato del Gestore della Segnalazione</u>	L'adozione di tali misure consente alla Società di limitare il numero di soggetti che hanno accesso ai dati personali.
	<u>Designazione dei soggetti autorizzati al trattamento; attività di formazione; adozione della Procedura Whistleblowing.</u>	L'adozione di tali misure consente alla Società di istruire in maniera dettagliata i soggetti coinvolti nei trattamenti.
Come stimereste la <u>gravità</u> del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	<input type="checkbox"/> Trascurabile <input checked="" type="checkbox"/> Limitata <input type="checkbox"/> Importante <input type="checkbox"/> Massimo	Tale stima è stata elaborata alla luce dei seguenti fattori: <ul style="list-style-type: none"> <li>- Presenza di procedure specifiche per l'archiviazione dei dati personali;</li> <li>- Presenza di specifici profili di autorizzazione in merito agli accessi ai dati personali.</li> </ul>
Come stimereste la <u>probabilità</u> del rischio, specialmente con riguardo alle minacce, alle fonti del rischio e alle misure pianificate?	<input type="checkbox"/> Trascurabile <input checked="" type="checkbox"/> Limitata <input type="checkbox"/> Importante <input type="checkbox"/> Massima	Le misure organizzative e tecniche di sicurezza adottate dalla Società consentono di stimare la probabilità del rischio derivante dalle fonti di cui sopra come limitata.

Il gestore della segnalazione

Avv. Marella Mazzei



IMPRESA COSTRUZIONI  
**GALLO - ROAD S.R.L.**  
 Via P. Maroncelli n. 23 - PADOVA  
 P. IVA 00220250288

23

C.F.O. (monitoraggio svolgimento della DPIA)

Dott. Giacomo Lorenzin

