



GRINDING TECHNOLOGY

meccanodora MORAS TACCHELLA

**TITOLARE WHISTLEBLOWING:**

Grinding Technology Srl  
Strada Statale Valle Bormida Nord 4  
15016 Cassine (AL)

**CLASSIFICAZIONE**

DATA: 16/12/2025


REV: 01



# Valutazione di impatto sulla protezione dei dati

**APPROVATO DA:**

.....  
(Timbro/Firma Titolare)

 <p>GRINDING TECHNOLOGY meccanodora ANNA TACCHELLA</p>	<p><b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)</p>	<p><b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01</p>
---	---	--

## 1) Scopo del documento e riferimenti normativi

Il presente documento risponde all'obbligo previsto dall'Art. 13(6) del D.Lgs.24/2023 e viene redatto in conformità all'Art.35 del Reg.UE 2016/679 "Valutazione d'impatto sulla protezione dei dati" (o Privacy Impact Assessment, di seguito anche PIA). Il presente documento contiene inoltre gli elementi di cui all'Art.30 del Reg.UE 2016/679 "Registri delle attività di trattamento". Il presente documento è pertanto da considerarsi come parte integrante di:

- Modello di ricevimento e gestione delle segnalazioni whistleblowing (al quale si rimanda per eventuali approfondimenti);
- Sistema di conformità privacy aziendale.

## 2) Definizione PIA

Una PIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono il Titolare del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento. In altre parole, una **valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità del trattamento**. La PIA può riguardare un singolo trattamento o trattamenti multipli simili tra di loro, in termini di natura, ambito di applicazione, contesto, finalità e rischi.

Di seguito l'infografica dell'Autorità Garante per la protezione dei dati riferita alla PIA

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7185457>

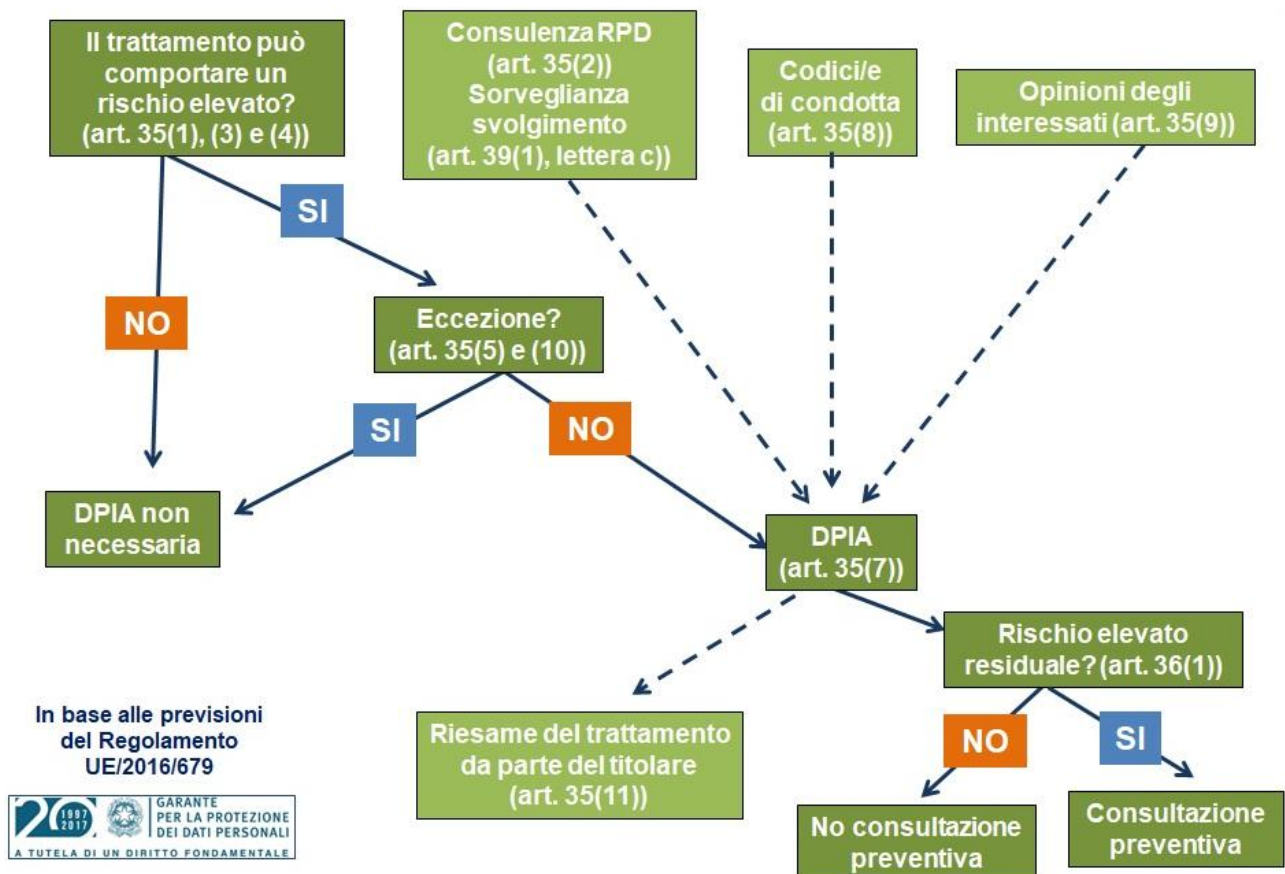
<p><b>COSA È?</b> È una procedura prevista dall'articolo 35 del Regolamento UE/2016/679 (RGPD) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.</p>	
<p><b>PERCHÉ?</b> La DPIA è uno strumento importante in termini di responsabilizzazione (<i>accountability</i>) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.</p>	<p><b>QUANDO LA DPIA È OBBLIGATORIA?</b> In tutti i casi in cui un trattamento può presentare un <b>rischio elevato per i diritti e le libertà</b> delle persone fisiche. Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito: - trattamenti valutativi o di <i>scoring</i>, compresa la profilazione; - decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni); - monitoraggio sistematico (es: videosorveglianza); - trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche); - trattamenti di dati personali su larga scala; - combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data); - dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.); - utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.); - trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento). La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.</p>
<p><b>IN CHE MOMENTO?</b> La DPIA deve essere condotta <b>prima</b> di procedere al trattamento. Dovrebbe comunque essere previsto un <b>riesame continuo</b> della DPIA, <b>ripetendo la valutazione a intervalli regolari</b>.</p>	<p><b>QUANDO LA DPIA NON È OBBLIGATORIA?</b> Secondo le Linee guida del Gruppo Art. 29, la DPIA <b>NON</b> è necessaria per i trattamenti che: - non presentano rischio elevato per i diritti e libertà delle persone fisiche; - hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA; - sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche; - sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA; - fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.</p>
<p><b>CHI?</b> La <b>responsabilità</b> della DPIA spetta al <b>titolare</b>, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare <b>ne monitora</b> lo svolgimento <b>consultandosi</b> con il <b>responsabile della protezione dei dati</b> (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del <b>responsabile della sicurezza dei sistemi informativi</b> (<i>Chief Information Security Officer, CISO</i>) e del <b>responsabile IT</b>.</p>	


## 2) Indicazioni legali sulla conduzione della PIA

La conduzione della PIA avviene secondo i seguenti riferimenti normativi:

- GDPR, Art.35 del Regolamento UE 2016/679 “Valutazione d'impatto sulla protezione dei dati”;
- GDPR, Considerando 84, 89-93, 95;
- Gruppo di lavoro Art.29 per la protezione dei dati (WP248 rev.01) “Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679” adottate il 04/05/2017 e modificate il 04/10/2017;
- Provvedimento dell’Autorità Garante Italiana N°467 del 11/10/2018 “Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell’art. 35, comma 4, del Regolamento (UE) n. 2016/679” pubblicato in Gazzetta Ufficiale N°269 del 19/11/2018;
- Linee guida destinate ai Responsabili della protezione dei dati per il rispetto del Regolamento generale sulla protezione dei dati dell’Unione Europea (versione approvata dalla Commissione, luglio 2019).

Di seguito l’infografica dell’Autorità Garante che presenta lo scenario di conduzione della PIA



 GRINDING TECHNOLOGY <small>meccanodora JONAS TACCHELLA</small>	<b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)	<b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01
--	---	---

### 3) Quando condurre una PIA

E' necessario condurre una PIA qualora:

- ricorra il criterio generale di rischio elevato previsto dall'Art.35, comma 1;
- ricorra almeno uno dei casi particolari previsti dall'Art.35, comma 3;
- ricorrano 2 o più criteri tra quelli previsti dal WP29;
- un trattamento soggetto al meccanismo di coerenza rientri nelle tipologie previste dall'All.1 del Provv. 467 del 11/10/2018.

**Criterio principale** La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4).

**Casi particolari** La PIA è richiesta in particolare nei casi seguenti:


- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

**Criteri previsti da WP29** La PIA è richiesta al ricorrere di 2 o più dei seguenti criteri:

- valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
- processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone;
- monitoraggio sistematico degli interessati;
- dati sensibili o dati aventi carattere altamente personale;
- trattamento di dati su larga scala;
- creazione di corrispondenze o combinazione di insiemi di dati;
- dati relativi a interessati vulnerabili;
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
- quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".

**Criteri previsti dal Garante Italiano** In caso di trattamenti soggetti al meccanismo di coerenza, la PIA è richiesta al ricorrere di almeno uno dei seguenti criteri:

- Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"
- Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)
- Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
- Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

 GRINDING TECHNOLOGY <small>meccanodora JONAS TACCHIELLA</small>	<b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)	<b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01
---	---	---

- 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 (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
- Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
- Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP248, rev. 01 .
- Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
- Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
- Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
- Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
- Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

## 4) Metodologia di conduzione della PIA

### 4.1) Tempistica

La PIA va effettuata "**prima del trattamento**", in coerenza con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita. La PIA va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento. La PIA è un **processo continuo**, soprattutto quando un trattamento è dinamico ed è soggetto a variazioni continue.

### 4.2) Soggetti

- Al **Titolare del trattamento** spetta assicurare che la PIA sia eseguita. La PIA può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito.
- Il Titolare deve consultare il **Responsabile della protezione dei dati** ed eventuali **Responsabili del trattamento**.
- E' consigliabile che il Titolare raccolga le opinioni **degli interessati o dei loro rappresentanti**.
- E' consigliabile che fornisca assistenza al Titolare il **capo della sicurezza dei sistemi di informazione (e/o il dipartimento IT)**.


### 4.3) Contenuti

Il GDPR definisce le caratteristiche minime dei contenuti di una PIA, che deve fornire almeno:

- una descrizione dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi e dimostrare la conformità al GDPR.

Di seguito l'infografica dell'Autorità Garante che presenta il processo di conduzione della PIA



 GRINDING TECHNOLOGY <small>meccanodora JONAS TACCHELLA</small>	<b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)	<b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01
--	---	---

#### 4.4) Conclusioni

All'esito della PIA il Titolare è tenuto a:


- procedere con il trattamento qualora la PIA indichi che il livello di rischio è correttamente attenuato da adeguate misure di sicurezza, che garantiscano un livello di rischio residuo accettabile;
- procedere con un riesame qualora insorgano variazioni negli elementi analizzati tramite la PIA;
- consultare l'autorità Garante ogni qualvolta non sia in grado di trovare misure sufficienti per ridurre i rischi ad un livello accettabile.

#### 5) La necessità di condurre una PIA in riferimento al Whistleblowing

Indipendentemente dai criteri di cui al Cap.3 "Quando condurre una PIA", nel caso in esame l'obbligo è sancito direttamente dal Legislatore, ai sensi dell'Art.13(6) del D.Lgs.24/2023 "Trattamento dei dati personali": *I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018.*

#### 6) Descrizione del trattamento

<b>Tipologia di dati trattati</b>	Sono trattati tutti i dati personali contenuti nel processo di segnalazione, nonché negli eventuali successivi approfondimenti di indagine. Tali dati possono essere qualificati come comuni (dati anagrafici) o relativi a reati (GDPR, Art.10). Di norma, a meno di dati inseriti volontariamente dal segnalante, si esclude il trattamento di dati appartenenti alle categorie particolari (GDPR, Art.9)
<b>Attività di trattamento</b>	In funzione degli obblighi normativi sono possibili i seguenti trattamenti: raccolta, registrazione, conservazione, consultazione, trasmissione, cancellazione
<b>Finalità del trattamento</b>	I dati sono trattati allo scopo di una corretta gestione delle segnalazioni, connessi adempimenti normativi, riscontri al segnalante ed eventuali approfondimenti di indagine.
<b>Base giuridica del trattamento</b>	La base giuridica del trattamento è da rinvenirsi nell'Art.6, comma1(c) "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare".
<b>Modalità e strumenti del trattamento</b>	I dati sono trattati secondo modalità e con strumenti atti a garantirne la massima sicurezza e riservatezza. L'identità del segnalante è protetta secondo le prescrizioni di cui all'Art. 12 del D.Lgs.24/2023 "Obbligo di riservatezza". La società ha adottato quale canale di segnalazione interno una piattaforma on-line, dotata dei necessari requisiti di sicurezza
<b>Conservazione dei dati</b>	I dati sono trattati per tempi compatibili con le prescrizioni normative, con specifico riferimento all'Art.14 del D.Lgs.24/2023 "Conservazione della documentazione inerente alle segnalazioni": le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque <b>non oltre cinque anni</b> a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. In caso di inserimento da parte dei segnalanti di dati manifestamente non utili alla gestione della segnalazione, il Gestore procederà all'immediata cancellazione, compatibilmente con i vincoli tecnici della piattaforma (in conformità all'Art.13(1) del Decreto 24/2023)
<b>Ambito di conoscibilità</b>	Potranno accedere ai dati esclusivamente soggetti formalmente designati, autorizzati ed istruiti, tra cui: gestore del canale di segnalazione, organi di controllo, gestori e collaboratori interni, ecc. In caso di indagini i dati potranno essere conosciuti dalle pubbliche autorità preposte. In generale i dati potranno essere conosciuti nell'ambito delle prescrizioni di cui all'Art.12 del D.Lgs.24/2023.

 GRINDING TECHNOLOGY <small>meccanodora ROMA TACCHELLA</small>	<b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)	<b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01
---	---	---

## 7) Aderenza ai principi generali

<b>Liceità</b>	Il trattamento viene effettuato nell'espletamento di un obbligo legale a cui è soggetto il Titolare.
<b>Limitazione della finalità</b>	Si esclude l'utilizzo dei dati per fini differenti rispetto agli adempimenti di legge.
<b>Minimizzazione</b>	La piattaforma è configurata con i campi necessari all'acquisizione dei dati indispensabili alla gestione delle segnalazioni. Il segnalante è tenuto ad inserire informazioni pertinenti (si diffondono dettagliate istruzioni in tal senso).
<b>Esattezza</b>	Il segnalante è tenuto a inserire informazioni di cui abbia ragionevole certezza (si diffondono dettagliate istruzioni in tal senso).
<b>Limitazione della conservazione</b>	Vedi paragrafo precedente (riga tabella "Conservazione dei dati")
<b>Integrità e riservatezza</b>	Vedi misure di sicurezza

## 8) Informazioni e diritti degli interessati

<b>Modalità di diffusione dell'informativa</b> (GDPR, Art.13)	Il Titolare ha adottato adeguati canali di diffusione delle istruzioni in merito a come effettuare una segnalazione: <ul style="list-style-type: none"> <li>⦿ pubblicazione istruzioni su proprio sito internet</li> <li>⦿ esposizione infografica presso sede</li> <li>⦿ consegna istruzioni ai dipendenti</li> <li>⦿ inserimento disclaimer email</li> </ul> Su proprio sito web è inoltre disponibile apposito documento contenente note legali ed informativa privacy riferita al trattamento dei dati contenuti nelle segnalazioni  Sul portale di segnalazione sono presenti ulteriori specifiche tecniche sui requisiti di sicurezza della piattaforma
<b>Modalità di garanzia di esercizio dei diritti degli interessati</b> (GDPR, Art.15-21)	Si segnala che i diritti di cui agli articoli da 15 a 22 del GDPR possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs.196/2003 "Limitazioni ai diritti dell'interessato", ossia rivolgendosi direttamente all'Autorità Garante.

## 9) Valutazione del rischio

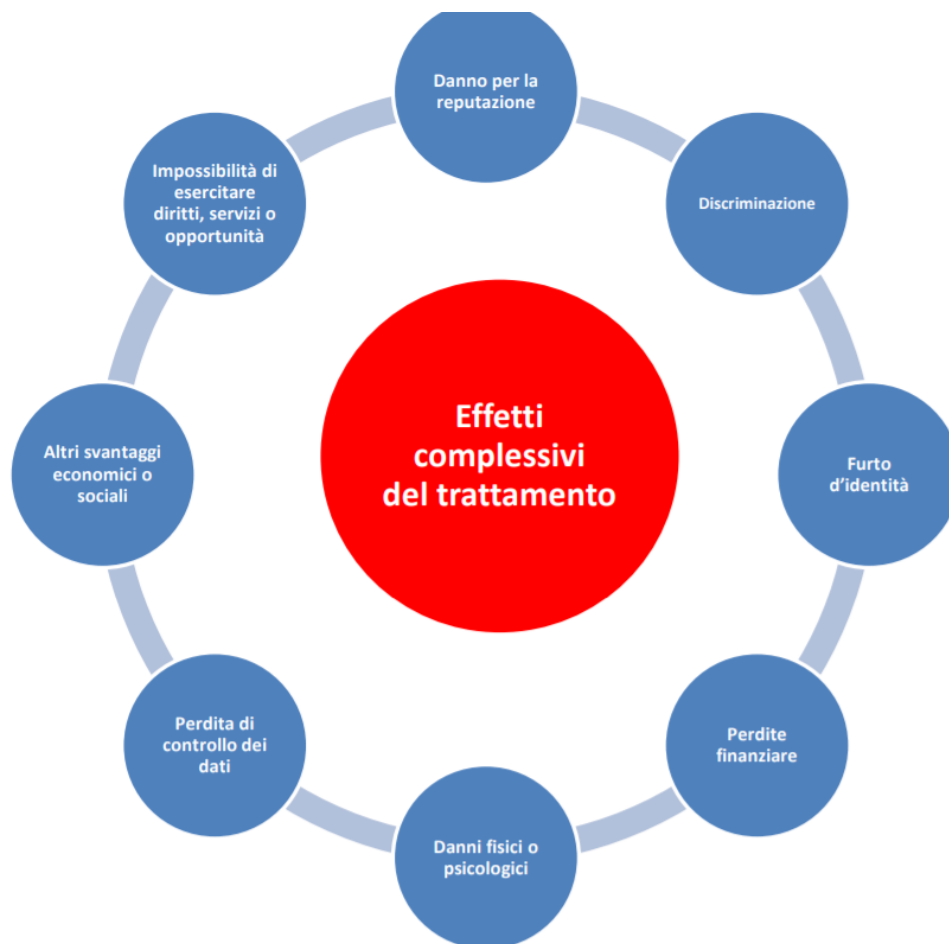
Al fine di identificare una corretta metodologia di analisi dei rischi, Il Titolare si base sulle indicazioni dell'Autorità Garante diffuse al seguente link: <http://www.garanteprivacy.it/regolamentoue/dpia/gestione-del-rischio>



Pertanto, preliminarmente alla definizione della metodologia occorre focalizzare il vero obiettivo dell'analisi di rischio prevista dal GDPR, ossia **l'impatto sui diritti e le libertà fondamentali delle persone fisiche**. Il legislatore focalizza dunque il processo sull'interessato, invitando a sensibilizzare il Titolare sulle possibili




conseguenze che i trattamenti effettuati possano generare sulle persone che hanno conferito tali dati (interessati). In particolare occorre identificare una metodologia che definisca quale livello di rischio per gli interessati possa derivare da un evento dannoso quale distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzato in funzione delle possibili conseguenze illustrate nella seguente figura.





La seguente tabella classifica una sintesi dei suddetti elementi in funzione del trattamento in oggetto.


RISCHIO	MINACCIA	PROB.	GRAV.	IMPATTO SUGLI INTERESSATI
Accesso illegittimo	Comportamento fraudolento degli operatori o soggetti esterni	BASSA	MEDIA	Potenziale utilizzo improprio dei dati; danni reputazionali, discriminazione
Modifica indesiderata	Comportamento fraudolento degli operatori o soggetti esterni	BASSA	MEDIA	Potenziale utilizzo improprio dei dati; danni reputazionali, discriminazione
Distruzione, perdita	Eventi distruttivi; errore umano	BASSA	BASSA	

Il sistema non risulta esposto ad eventuali ulteriori impatti negativi per l'interessato quali: danni fisici o fisiologici, furto di identità, perdita di controllo dei dati, ecc.

 GRINDING TECHNOLOGY meccanodora ANISA TACCHELLA	<b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)	<b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01
---	---	---

## 10) Misure di sicurezza e rischio residuo

<b>Accesso ai dati</b>	<ul style="list-style-type: none"> <li>Al fine di limitare il rischio di utilizzo improprio del sistema, il Titolare ha optato per una gestione interamente esternalizzata, basata sul supporto di fornitori qualificati e su strumenti certificati.</li> <li>Tutti i soggetti che possono accedere ai dati sono regolarmente designati ed istruiti.</li> <li>Il gestore del canale di segnalazione comunica l'identità del segnalante solo nei casi espressamente previsti dalla legge</li> <li>E' possibile effettuare segnalazioni in forma anonima</li> <li>Lo sviluppatore della piattaforma non ha alcuna forma di accesso ai dati, che risultano conservati in modalità crittografata</li> <li>Il sistema mette a disposizione del segnalante appositi codici di accesso alla propria segnalazione</li> </ul>
<b>Sicurezza della piattaforma</b>	<p>Si è attivato un canale di segnalazione dotato dei requisiti software ed hardware richiesti.</p> <p><b>Requisiti software</b></p>  <p>Conforme allo standard ISO 37002, alla Direttiva UE 2019/1937 e al Regolamento generale sulla protezione dei dati (GDPR). L'applicativo è stato adottato in tutto il mondo, in oltre 10.000 progetti di Whistleblowing.</p> <p>A garanzia della conformità e dell'affidabilità della soluzione, segnaliamo che, in Italia, <u>l'applicativo è utilizzato per lo sviluppo del canale Whistleblowing dell'ANAC</u> (Autorità Nazionale Anti Corruzione), il soggetto che presidia l'applicazione della norma. Sul portale web globaleaks (<a href="https://www.globaleaks.org/">https://www.globaleaks.org/</a>) è possibile approfondire:</p> <ul style="list-style-type: none"> <li>il profilo e la storia del team di sviluppo;</li> <li>le caratteristiche tecniche, legali e di sicurezza del software;</li> <li>la documentazione tecnica a corredo.</li> </ul> <p><b>Requisiti hardware</b></p> <p>L'applicativo Globaleaks è ospitato in un ambiente dedicato, collocato in un datacenter italiano, dotato delle massime garanzie di affidabilità (<a href="https://www.naquadria.it/il-datacenter">https://www.naquadria.it/il-datacenter</a>)</p>  <p>La configurazione del servizio garantisce la completa separazione logica degli ambienti, che saranno raggiungibili mediante URL dedicato su dominio di terzo livello.</p>
<b>Valutazione finale sul rischio residuo</b>	<b>In riferimento all'analisi dei rischi ed alle misure di sicurezza adottate il rischio residuo legato al trattamento risulta: ACCETTABILE</b>

 <b>GRINDING TECHNOLOGY</b> <small>meccanodora JONAS TACCHELLA</small>	<b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)	<b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01
---	---	---


Nell'adozione delle suddette misure si è tenuto in debita considerazione il contenuto dell' Art.13 del Decreto Whistleblowing "Trattamento dei dati personali" prescrive che:

1. *Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto, deve essere effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51. La comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea è effettuata in conformità del regolamento (UE)2018/1725.*
2. *I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.*
3. *I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2 -undecies del decreto legislativo 30 giugno 2003, n. 196.*
4. *I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati dai soggetti di cui all'articolo 4, in qualità di titolari del trattamento, nel rispetto dei principi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679 o agli articoli 3 e 16 del decreto legislativo n. 51 del 2018, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.*
5. *I soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni, ai sensi dell'articolo 4, comma 4, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del regolamento (UE) 2016/679 o dell'articolo 23 del decreto legislativo n. 51 del 2018.*
6. *I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018.*

## 11) Consultazione delle parti

Nello sviluppo del Modello di gestione delle segnalazioni il Titolare ha consultato i seguenti soggetti:

- Gestore del canale di segnalazione
- Gestore e Collaboratore interno
- Organismo di vigilanza / altro organo di controllo

 <b>GRINDING TECHNOLOGY</b> <small>meccanodora ADRIANA TACCHELLA</small>	<b>TITOLARE WHISTLEBLOWING:</b> Grinding Technology Srl Strada Statale Valle Bormida Nord 4 15016 Cassine (AL)	<b>CLASSIFICAZIONE</b> DATA: 16/12/2025 REV: 01
---	---	---

## 12) Esito della valutazione di impatto

La seguente tabella riassume le conclusioni della valutazione di impatto condotta, definendo la conformità normativa (o la necessità di consultazione preliminare dell’Autorità Garante) del trattamento in oggetto.

OBIETTIVO DI ANALISI	RISULTATO	NOTE
Il trattamento è basato su di un corretto principio di liceità?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	GDPR, Art.6 (c)
La finalità è determinata, esplicita e legittima?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	Adempimenti di legge
I dati trattati sono adeguati, pertinenti e limitati?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	
I dati sono conservati per tempi coerenti con la finalità della raccolta?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	
I soggetti esterni coinvolti nel trattamento prestano adeguate garanzie?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	
I trasferimenti all’estero avvengono conformità al Capo V del GDPR?	<input type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input checked="" type="radio"/> N/A	
Sono fornite adeguate informazioni agli interessati?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	
Gli interessati possono esercitare i diritti di cui agli art.15-21 del GDPR?	<input type="radio"/> <b>Si</b> <input checked="" type="radio"/> <b>No</b> <input type="radio"/> N/A	Diritto limitato da Decreto
I rischi per i diritti e le libertà fondamentali degli interessati sono adeguatamente analizzati?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	
Le misure di sicurezza poste a tutela dei dati sono in grado di limitare i rischi ad un livello residuo accettabile?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	
Sono state consultate le parti coinvolte nel processo di trattamento?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	
Le parti coinvolte nel processo di trattamento concordano con le valutazioni di impatto?	<input checked="" type="radio"/> <b>Si</b> <input type="radio"/> <b>No</b> <input type="radio"/> N/A	

## CONCLUSIONE DELLA VALUTAZIONE DI IMPATTO

**Il trattamento in oggetto può iniziare/proseguire**

(il livello di rischio è correttamente attenuato da adeguate misure di sicurezza, che garantiscano un livello di rischio residuo accettabile)

La presente valutazione di impatto sarà oggetto di opportuna revisione qualora intercorressero significativi cambiamenti nei profili oggetto di analisi.