



# Corporate Policy

Policy di gestione delle segnalazioni -  
whistleblowing  
Whistleblowing Policy

IT-EN

A digital and updated version of this document is  
always available in the



**QMS Factory Portal**

MAN\_whistleblowing - Rev.1.7 of 30/04/2026  
IMA Group Quality Management System  
QMS Factory Folder N. 2022\_1



COMPLIANCE 231



**VALIDO DAL / VALID FROM 30/04/2026**

## **AMBITO DI APPLICAZIONE / FIELD OF APPLICATION**

Il documento trova applicabilità: / *This Document is applicable to:*



Nelle Società dotate di Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001, come indicato nella Matrice dei contesti. / *Companies that have adopted an Organizational, Management and Control Model pursuant to Italian Legislative Decree 231/2001, as indicated in the Contexts matrix.*

Per contesto si intende l'insieme dei fattori significativi per la conformità sia ai requisiti cogenti applicabili sia a quelli definiti dall'Alta Direzione.

Il **contesto principale** del presente documento è Compliance 231. / *Context means the set of issues that are relevant to the compliance with both the applicable mandatory requirements and the requirements defined by Top Management. The **principal context** of this document is Compliance 231.*

Questo documento è valido nelle seguenti Divisioni/Società del Gruppo IMA: / *This document is valid in the following Divisions/Companies of the IMA Group:*

1. IMA S.p.A.
2. CO.MA.DI.S. S.p.A.
3. PHARMASIENA SERVICE S.r.l.
4. ILAPAK ITALIA S.p.A.
5. EUROSICMA S.p.A.
6. PETRONCINI IMPIANTI S.p.A.
7. SPREAFICO AUTOMATION S.r.l.
8. CIEMME S.r.l.
9. TISSUE MACHINERY COMPANY S.p.A.
10. ATOP S.p.A.
11. Teknoweb Converting S.r.l.
12. Mesplic S.r.l.
13. OMAS Tecnosistemi S.p.A.
14. IMA Sarong S.r.l.
15. Record S.p.A.
16. Perfect Pack S.r.l.
17. Spares Service & Machinery S.r.l.
18. ALPHAMAC S.r.l.
19. Benhil GmbH
20. Erca France S.A.S.
21. GASTI Verpackungsmaschinen GmbH
22. Hassia Verpackungsmaschinen GmbH
23. INTECMA S.A.



Questo documento è stato approvato tramite firma elettronica all'interno del sito Quality&Compliance di SharePoint, in cui sono archiviati anche lo storico delle modifiche e dei flussi approvativi. / *This document has been approved by electronic signature in SharePoint Quality&Compliance site, in which the version history of changes and the approvals workflows are archived.*

Each printed copy of this document, must be considered as UNCONTROLLED COPY OF WORK, the current version is available in electronic form in the intranet "QMS Factory" of the IMA Group.



## INDICE / INDEX

VERSIONE ITALIANA .....	6
SCOPO DEL DOCUMENTO .....	6
RISCHI DI PROCESSO.....	6
TERMINI E DEFINIZIONI .....	7
RIFERIMENTI NORMATIVI.....	8
1. AMBITO DI APPLICAZIONE .....	10
1.1. Soggetti coinvolti.....	10
2. MODALITA' DI SEGNALAZIONE.....	11
2.1. Forma scritta .....	11
2.2. Forma orale o verbale .....	12
2.3. Canale esterno.....	12
3. LA SEGNALAZIONE.....	13
4. GESTIONE DELLE SEGNALAZIONI.....	14
4.1. Protocollo e custodia.....	15
4.2. Istruttoria ("Triage").....	16
4.3. Indagine di merito .....	16
4.4. Archiviazione .....	17
5. RISERVATEZZA E TRATTAMENTO DEI DATI PERSONALI .....	17
6. DIVIETO DI RITORSIONI E MISURE DI SOSTEGNO E PROTEZIONE DEL SEGNALANTE .....	18
7. ATTIVITA' INFORMATIVA.....	20
ALLEGATO 1 - Informativa ai sensi degli art. 13-14 GDPR.....	21
ENGLISH VERSION.....	24
DOCUMENT PURPOSE .....	24
PROCESS RISKS .....	24
TERMS AND DEFINITIONS.....	25
STANDARD REFERENCES .....	26
1. FIELD OF APPLICATION .....	27
1.1. Involved subjects.....	27
2. REPORTING METHODS .....	28
2.1. Written form .....	28



2.2	Oral or verbal form.....	29
2.3	External channel.....	29
3.	WHAT CAN BE REPORTED .....	30
4.	MANAGEMENT OF REPORTS.....	32
4.1	Protocol and custody.....	32
4.2	Preliminary investigation (“Triage”).....	33
4.3	Substantive investigation .....	33
4.4	Archiving.....	34
5.	PRIVACY AND PROSESSING OF PERSONAL DATA.....	34
6.	PROHIBITION OF RETALIATION AND SUPPORT AND PROTECTION MEASURES FOR THE WHISTLEBLOWER .....	35
	ANNEX 1 – INFORMATION pursuant art. 13-14 GDPR.....	38
	APPROVAZIONE ELETTRONICA DEL DOCUMENTO/ ELECTRONIC APPROVAL OF THE DOCUMENT ...	40
	<i>STORICO REVISIONI (VERSION HISTORY)</i> .....	41

Each printed copy of this document, must be considered as UNCONTROLLED COPY OF WORK, the current version is available in electronic form in the intranet "QMS Factory" of the IMA Group.

## **VERSIONE ITALIANA**

### **SCOPO DEL DOCUMENTO**

Il "**whistleblowing**" è il termine che identifica una segnalazione compiuta da un soggetto che, nello svolgimento delle proprie mansioni, si accorge di un illecito, un rischio o una situazione di pericolo che possa arrecare danno all'azienda per cui lavora, nonché a clienti, colleghi, cittadini e qualunque altra categoria di soggetti.

IMA, sensibile alle tematiche etiche e di corretta condotta del proprio business, ha implementato un **sistema** atto a ricevere e gestire segnalazioni di azioni, fatti o situazioni che possano costituire condotte illecite rispetto a:

- legislazione vigente;
- Codice Etico;
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01;
- Sistema di Gestione della Sicurezza sul Lavoro;
- Sistema di Gestione Ambientale;
- Presunte violazioni di normative e leggi nello svolgimento delle attività lavorative che possano arrecare danno o pregiudizio, anche solo d'immagine, alla Società.
- Regolamento UE 679/2016 (GDPR)

La Policy Whistleblowing adottata da IMA intende:

- **garantire** la riservatezza del segnalante e nello spirito della norma, tutelare quest'ultimo da possibili ritorsioni;
- **promuovere** una cultura fondata sulla responsabilità e sull'etica;
- **consentire** agli Organi Sociali e di Controllo di IMA di essere informati su fatti o condotte contrarie ai principi etici adottati, al fine di individuare e gestire possibili carenze nel sistema di controllo interno e di gestione dei rischi;
- **fornire** le linee guida per effettuare e gestire le segnalazioni in maniera efficace, responsabile e in conformità con la Legge.

### **RISCHI DI PROCESSO**



La metodologia per identificare i rischi e valutare le aree maggiormente esposte alla commissione dei reati 231 è documentata nella WI\_27.2.



## TERMINI E DEFINIZIONI

<b>Canale Interno</b>	Si intende lo strumento adottato da IMA e dalle società del Gruppo IMA soggette alla Direttiva EU 2019/1937 per consentire l’inoltro di segnalazioni di possibili violazioni di leggi, regolamenti, norme o procedure. Il canale interno adottato da IMA e dalle società del Gruppo IMA garantisce tramite l'applicazione di strumenti di crittografia, la riservatezza dell’identità del Segnalante e dei relativi dati personali, nonché del contenuto della Segnalazione e dei relativi documenti
<b>D. Lgs. 24/2023</b>	Si intende il Decreto Legislativo 10 marzo 2023 n. 24 <i>“Attuazione della Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019, riguardante la “Protezione delle persone che segnalano violazioni del Diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”</i>
<b>Direttiva UE 2019/1937</b>	Si intende la Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019, riguardante la <i>“Protezione delle persone che segnalano violazioni del Diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”</i>
<b>Domicilio del Gestore delle Segnalazioni</b>	Si intende il domicilio eletto dal Gestore delle Segnalazioni presso IMA S.p.A., Via Emilia 428/442, Ozzano dell’Emilia (BO)
<b>Facilitatore</b>	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.
<b>Gruppo IMA – Gruppo</b>	Indica la stessa IMA S.p.A. e l’insieme delle società controllate, direttamente o indirettamente, da IMA S.p.A. ai sensi dell’art. 2359 c.c.
<b>IMA o Società</b>	IMA S.p.A. – Via Emilia, 428/442 - 40064 Ozzano dell’Emilia (BO) Italy, Codice Fiscale 00307140376 e Partita IVA 00500931209.
<b>Gestore delle Segnalazioni</b>	È il comitato responsabile della gestione delle Segnalazioni Riservate per IMA S.p.A. e per le società del Gruppo IMA (in quest’ultimo caso il Gestore delle Segnalazioni opera ai sensi dell’art. 5 del D. Lgs. 24/2023). Gestisce ed è responsabile della corretta gestione del Canale Interno, della fase di Istruttoria (“Triage”) e dell’Indagine di Merito (investigazione). Il Gestore delle Segnalazioni è costituito da un comitato composto da tre professionisti indipendenti ed autonomi con competenze trasversali in materia legale e di compliance.
<b>Leggi di Recepimento</b>	Si intendono le leggi nazionali di recepimento della Direttiva EU 2019/1937.
<b>Segnalante o Whistleblower</b>	È il soggetto che effettua una segnalazione.



4.0

<b>Segnalazione</b>	Comunicazione di qualsiasi violazione delle norme che possa avere impatto sulla Società resa secondo i termini della presente Policy e nel rispetto dei principi e delle regole stabilite dal D. Lgs 24/2023.
<b>Ritorsione</b>	Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione o della denuncia o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.
<b>Segnalato</b>	Si intende colui che è oggetto della Segnalazione
<b>MyWhistleblowing IMA</b>	Piattaforma dedicata alla gestione delle Segnalazioni Riservate secondo le prescrizioni del D. Lgs. 24 del 10 marzo 2023. Alla piattaforma MyWhistleblowing IMA si può accedere tramite il sito web <a href="http://www.imagroup.com">www.imagroup.com</a> oppure tramite la intranet MyIMA oppure direttamente al seguente indirizzo: <a href="https://areariservata.mygovernance.it#!/WB/IMASPA">https://areariservata.mygovernance.it#!/WB/IMASPA</a> per segnalazioni riguardanti IMA S.p.A.; <a href="https://areariservata.mygovernance.it#!/WB/IMA-Controllate-Italia">https://areariservata.mygovernance.it#!/WB/IMA-Controllate-Italia</a> per segnalazioni riguardanti le società italiane appartenenti al Gruppo IMA che sono soggette alla normativa; <a href="https://areariservata.mygovernance.it#!/WB/IMA-Europe">https://areariservata.mygovernance.it#!/WB/IMA-Europe</a> per segnalazioni riguardanti le società europee appartenenti al Gruppo IMA che sono soggette alla normativa.
<b>Organo societario competente</b>	Si intende l'Organo Sociale, l'Organismo o l'Ufficio a cui il Gestore delle Segnalazioni riporta il risultato delle attività svolte. È il soggetto responsabile, per competenza, dell'adozione di eventuali misure di rimedio o dell'erogazione di azioni correttive.
<b>Società del Gruppo IMA</b>	Si intende IMA S.p.A. e qualsiasi società da questa controllata interessata dalla Direttiva UE 2019/1937

## RIFERIMENTI NORMATIVI

La presente Policy è stata redatta facendo riferimento a:

- **Decreto Legislativo n. 24 del 10/3/2023** – Attuazione della Direttiva UE 2019/1937 riguardante la protezione delle persone che segnalano violazioni del Diritto dell'Unione e delle normative nazionali, ed in generale le Leggi di Recepimento di volta in volta applicabili a seconda della Società del Gruppo IMA coinvolta;
- **Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01** relativo alla Responsabilità Amministrativa degli Enti di IMA;
- **Regolamento UE 679/2016 (GDPR)**.



Per quanto non trattato esplicitamente dalla presente Policy e/o per l'interpretazione si fa riferimento al D. Lgs. 24/2023 e, laddove applicabili, alle altre normative di attuazione vigenti negli Stati membri in cui hanno sede le Società del Gruppo IMA.

Each printed copy of this document, must be considered as UNCONTROLLED COPY OF WORK, the current version is available in electronic form in the intranet "QMS Factory" of the IMA Group.



## 1. AMBITO DI APPLICAZIONE

La presente Policy **trova applicazione** sia in I.M.A. Industria Macchine Automatiche S.p.A. sia in tutte le società da essa, direttamente od indirettamente, controllate e facenti parte del “Gruppo IMA”, soggette alla Direttiva EU 2019/1937.

Con riferimento alle altre Società del Gruppo IMA con sede al di fuori dell’Unione Europea, qualora IMA, in qualità di capogruppo, dovesse ricevere una segnalazione, provvederà a gestirla nel rispetto della normativa locale applicabile e, laddove compatibile, in conformità con le procedure descritte nel presente documento.

Nella presente Policy sono individuati:

- i soggetti che possono attivare una segnalazione;
- gli atti o i fatti che possono essere oggetto di segnalazione, nonché i requisiti che le segnalazioni devono prevedere per poter essere prese in considerazione;
- le modalità attraverso cui segnalare le presunte violazioni e i soggetti preposti alla ricezione delle segnalazioni;
- il processo di istruttoria ed eventualmente di investigazione nel momento in cui viene effettuata una segnalazione;
- i protocolli attivati per garantire la riservatezza dei dati personali del/della Segnalante e della fattispecie oggetto di segnalazione;
- i protocolli attivati per garantire la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto eventualmente segnalato;
- i protocolli attivati per garantire il divieto di ritorsioni e il divieto di discriminazione nei confronti del soggetto Segnalante.

Il documento ha, infine, l'obiettivo di garantire che le attività di **gestione della Segnalazione siano svolte nel rispetto dei principi di professionalità, trasparenza e correttezza**, in conformità a quanto previsto dal DL 24/2023 (Decreto Legislativo in materia di whistleblowing) e più in generale alle Leggi ed ai regolamenti applicabili, nonché nel rispetto del Codice Etico aziendale, del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001.

### 1.1. Soggetti coinvolti

Il soggetto responsabile della gestione del Canale Interno di ogni Società del Gruppo IMA è il **Gestore delle Segnalazioni**, espressamente incaricato da ognuna delle suddette Società ed autorizzato allo svolgimento delle attività ritenute necessarie per l’assolvimento dei compiti attribuiti dal Dlgs 24/2023, dalle altre Leggi di Recepimento e dalla presente Policy. Il Gestore delle Segnalazioni è costituito da un **comitato** composto da tre professionisti indipendenti ed autonomi con competenze trasversali in materia legale e di compliance. Ai fini della presente Policy, il comitato che costituisce il Gestore delle Segnalazioni deve garantire, nel suo funzionamento, autonomia, indipendenza, professionalità e competenza specifica.

Il Gestore delle Segnalazioni potrà avvalersi del supporto di strutture interne di ciascuna società del Gruppo IMA ritenute maggiormente competenti rispetto alla fattispecie oggetto di segnalazione.



4.0

Nel caso di **conflitto di interessi**, ossia quelle fattispecie in cui il Gestore della Segnalazione coincida con il Segnalante, con il segnalato o sia comunque una persona coinvolta o interessata dalla Segnalazione (tale conflitto può, ad. es, sussistere anche rispetto al soggetto esterno, nel caso in cui la gestione della piattaforma sia esternalizzata), la Segnalazione dovrà essere indirizzata ad uno dei membri del Comitato Direttivo di IMA S.p.A., tramite informativa inviata a IMA S.p.A., Via Emilia 428/442, Ozzano dell'Emilia (BO), in busta chiusa e riservata all'attenzione del Comitato Direttivo nella persona del membro prescelto, il quale avrà cura di condividerne il contenuto con i membri del Gestore delle Segnalazioni non interessati dalla Segnalazione.

Resta fermo il diritto di optare per effettuare la Segnalazione cd. “esterna” ai sensi dell'art. 6 del D. Lgs. 24/2023.

Ai sensi dell'art. 4, sesto comma, del D. Lgs. 24/2023, qualora la Segnalazione dovesse essere comunicata ad un soggetto diverso dal Gestore delle Segnalazioni (ad es. all'Organismo di Vigilanza od al Collegio Sindacale), quest'ultimo la dovrà inoltrare al Gestore delle Segnalazioni entro sette giorni dalla ricezione, informandone contestualmente il Segnalante.

**I soggetti che posso effettuare una Segnalazione** sono i seguenti (“Segnalanti”):

- i componenti degli organi sociali (Assemblea, Consiglio di Amministrazione, Collegio Sindacale etc.);
- il personale (compresi dipendenti in forza, ex dipendenti, lavoratori temporanei, apprendisti, tirocinanti o volontari in relazione a circostanze avvenute durante il rapporto di lavoro o il processo di selezione);
- i soggetti esterni che intrattengono rapporti con le Società del Gruppo IMA (i cd. stakeholders come soci, clienti, fornitori, agenti, soci in affari, partner, appaltatori, subappaltatori, nonché collaboratori e dipendenti dei soggetti citati).

## 2. MODALITA' DI SEGNALAZIONE

Ogni società del Gruppo IMA si è dotata di un **Canale Interno** dedicato alle Segnalazioni, attivabile tramite le modalità sotto descritte.

### 2.1. Forma scritta

- a) **Piattaforma “MyWhistleblowing IMA”**, raggiungibile tramite il sito web [www.imagroup.com](http://www.imagroup.com) oppure tramite la intranet MyIMA oppure direttamente al seguente indirizzo:

<https://areariservata.mygovernance.it/#!/WB/IMAS.P.A.> per segnalazioni riguardanti IMA S.p.A.;

<https://areariservata.mygovernance.it/#!/WB/IMA-Controllate-Italia> per segnalazioni riguardanti le società italiane appartenenti al Gruppo IMA che sono soggette alla normativa.

<https://areariservata.mygovernance.it/#!/WB/IMA-Europe> per segnalazioni riguardanti le società europee appartenenti al Gruppo IMA che sono soggette alla normativa.



La piattaforma è estranea rispetto ai server aziendali, è gestita attraverso tecnologie cloud ed è dotata di strumento di crittografia che garantisce la riservatezza dell'identità del segnalante.

L'accesso alla piattaforma è consentito previa registrazione dell'utente e formale presa visione dell'informativa privacy e della procedura operativa.

L'accesso in forma anonima è consentito

- b) **A mezzo servizio postale in busta chiusa** (raccomandata) all'indirizzo del Gestore delle Segnalazioni IMA, domiciliato presso IMA S.p.A., Via Emilia 428/442, 40064 Ozzano dell'Emilia (BO), indicando espressamente sull'involucro "Segnalazione whistleblowing"

## 2.2. Forma orale o verbale

Tramite segnalazione verbale sul sistema di messaggistica disponibile all'interno della piattaforma MyWhistleblowing in cui è attivato un sistema di messaggistica vocale e testo. È possibile, inoltre, richiedere un **colloquio personale e riservato** con il Gestore delle Segnalazioni. Qualora la segnalazione riguardi una Società del Gruppo IMA con sede in un Paese diverso dall'Italia, il Gestore delle Segnalazioni si farà assistere nel corso del colloquio che resterà comunque personale e riservato da un soggetto interno o esterno della Società coinvolta, che parli la lingua madre del Segnalante ("Referente Locale"). Resta inteso che il Referente Locale deve possedere le caratteristiche di professionalità, indipendenza ed autonomia richieste dalla normativa applicabile.

**Non rientrano** nella presente Policy e conseguentemente non possono godere delle tutele previste dalle leggi applicabili, le segnalazioni o informazioni pervenute tramite email ordinaria, pec, o consegnate in modo difforme rispetto a quanto sopra previsto.

## 2.3. Canale esterno

Per quanto riguarda le Società del Gruppo IMA con sede in Italia, come previsto dal D. Lgs. n. 24 del 10 marzo 2023, l'Autorità Nazionale Anticorruzione (ANAC) ha attivato un **Canale di Segnalazione "Esterno"** a cui il Segnalante può effettuare una Segnalazione se, al momento della sua presentazione, ricorre una delle seguenti **condizioni**:

- a) non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del Canale interno di Segnalazione ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dall'articolo 4 del Decreto;
- b) il Segnalante ha già effettuato una Segnalazione attraverso il Canale interno di Segnalazione ai sensi dell'articolo 4 del Decreto e la stessa non ha avuto seguito;
- c) il Segnalante ha fondati motivi di ritenere che, se effettuasse una Segnalazione attraverso il Canale interno di Segnalazione, alla stessa non sarebbe dato efficace seguito ovvero che la stessa Segnalazione possa determinare il rischio di ritorsione;
- d) il Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Per quanto riguarda le Società del Gruppo IMA con sede in un Paese diverso dall'Italia, al ricorrere delle condizioni di cui sopra, le Segnalazioni Esterne potranno essere effettuate alle autorità competenti designate dallo Stato membro in cui ha sede la Società coinvolta, ai sensi



dell'articolo 11 della Direttiva UE 2019/1937.

### 3. LA SEGNALAZIONE

Può essere oggetto di **segnalazione interna** – attraverso, cioè, il canale whistleblowing che IMA ha deciso di adottare (v. par. 2.1 e 2.2 della presente Policy) – qualsiasi comportamento, atto od omissione che leda l'interesse pubblico o l'integrità di IMA e/o di una Società del Gruppo IMA e che integri (o si ritiene fondatamente che integri):

- a) un c.d. reato presupposto, già rilevante ai sensi del D. Lgs. n. 231/2001 (fatto salvo per quelle società del Gruppo IMA che non hanno adottato un proprio modello organizzativo di gestione e controllo ai sensi del D. Lgs. n. 231/2001);
- b) una violazione Modello Organizzativo di Gestione e Controllo adottato da IMA ai sensi del D. Lgs. n. 231/2001 (fatto salvo per quelle società del Gruppo IMA che non hanno adottato un proprio modello organizzativo di gestione e controllo ai sensi del D. Lgs. n. 231/2001);
- c) una violazione delle norme comunitarie e nazionali in materia di
  - appalti pubblici
  - servizi, prodotti e mercati finanziari
  - prevenzione del riciclaggio e del finanziamento del terrorismo
  - sicurezza e conformità dei prodotti
  - tutela dell'ambiente
  - radioprotezione e sicurezza nucleare
  - sicurezza degli alimenti e dei mangimi
  - salute e benessere degli animali
  - salute pubblica
  - protezione dei consumatori
  - tutela della vita privata e protezione dei dati personali
  - sicurezza delle reti e dei sistemi informativi
- d) una violazione delle norme comunitarie a protezione e garanzia degli interessi finanziari dell'Unione europea;
- e) una violazione delle norme comunitarie poste a protezione e garanzia della concorrenza e della libera circolazione di merci, persone, servizi e capitali all'interno del mercato comune europeo;
- f) una pratica (non inosservante, ma) comunque elusiva delle norme comunitarie di cui ai precedenti punti c), d) ed e);
- g) una violazione o una carenza concernente il sistema di gestione per la prevenzione della corruzione adottato dal Gruppo IMA.

In presenza delle condizioni già indicate al paragrafo 2.3 della presente Policy, solo le violazioni rilevanti ai sensi del D. Lgs. n. 24/2023, ovvero quelle sopra elencate alle lettere da a) a f), possono essere oggetto anche di **segnalazione esterna** (attraverso, cioè, il canale whistleblowing predisposto da ANAC).



In ogni caso, il D. Lgs. n. 24/2023 prevede espressamente che non possano essere oggetto di segnalazione – né attraverso il Canale Interno, né attraverso quello esterno predisposto da ANAC – le mere “irregolarità”, cioè quei comportamenti impropri che non arrivano però ad integrare un reato o una violazione delle normative sopra elencate.

La Segnalazione **deve essere adeguatamente circostanziata**<sup>1</sup> e resa con dovizia di particolari, con elementi tali da far emergere fatti e situazioni riferibili a contesti determinati ed avvenuti in ambito lavorativo, precisando che non vengono raccolti dati personali ulteriori rispetto a quelli strettamente necessari per la gestione della segnalazione stessa e che, in caso di raccolta accidentale, questi saranno immediatamente cancellati dal Gestore delle Segnalazioni. Il Segnalante è tenuto quindi a fornire tutti gli elementi disponibili e utili a consentire al Gestore delle Segnalazioni di procedere alle dovute ed appropriate verifiche e agli accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione, quali in via non esaustiva:

- i. una chiara e completa descrizione dei fatti oggetto della segnalazione;
- ii. le circostanze di tempo e di luogo in cui sono stati commessi i fatti oggetto della segnalazione;
- iii. le generalità o altri elementi che consentano di identificare il/i soggetto/i che ha/hanno posto in essere i fatti segnalati (ad es. qualifica, sede di servizio in cui svolge l’attività);
- iv. gli eventuali documenti a supporto della Segnalazione;
- v. ogni altra informazione che possa fornire utile riscontro circa la sussistenza dei fatti segnalati.

Nel campo di applicazione della presente Policy **non sono invece ricomprese**:

- segnalazioni su situazioni di carattere personale aventi ad oggetto rivendicazioni o rimostranze relative ai rapporti con i superiori gerarchici o con i colleghi, nonché relative all’esecuzione della propria prestazione lavorativa;
- segnalazioni fondate su meri sospetti o voci inerenti fatti personali non costituenti illecito: ciò in quanto è necessario sia tenere conto anche dell’interesse dei terzi oggetto delle informazioni riportate nella segnalazione, sia evitare che la Società svolga attività ispettive interne che rischiano di essere poco utili e comunque dispendiose.

Le segnalazioni anonime saranno prese in considerazione esclusivamente in presenza di tutti gli elementi che possano consentire al Gestore delle Segnalazioni di procedere ad una autonoma indagine; in caso contrario verranno archiviate.

## 4. GESTIONE DELLE SEGNALAZIONI

---

<sup>1</sup> Una segnalazione può ritenersi circostanziata se consente di individuare elementi di fatto ragionevolmente sufficienti per avviare un’indagine (ad es.: l’illecito commesso, il periodo di riferimento ed eventualmente il valore, le cause e la finalità dell’illecito, la società/divisione interessata, le persone/unità coinvolte, l’anomalia sul sistema di controllo).



Una volta ricevuta la Segnalazione secondo il Canale Interno previsto nella presente Policy attraverso le modalità scritte o verbali descritte nel paragrafo precedente, la gestione della stessa è articolata nelle seguenti fasi:

#### **4.1. Protocollo e custodia**

Nel caso la Segnalazione venga effettuata tramite accesso alla **piattaforma web MyWhistleblowing IMA**, è la piattaforma stessa a gestire la fase di protocollo tramite sistema di crittografia ed emissione di un codice identificativo unico in conformità con la normativa di riferimento.

La chiave di crittografia è custodita dal Gestore delle Segnalazioni che potrà utilizzarla solo ed esclusivamente con il consenso espresso e formale del Segnalante o su ordine dell'Autorità Giudiziaria competente.

Al ricevimento della Segnalazione, **non oltre 7 giorni dalla data di ricezione**, il Gestore delle Segnalazioni, tramite la piattaforma, invia una comunicazione di avvenuta ricezione e presa in carico della Segnalazione. La comunicazione viene inviata attraverso una comunicazione crittografata.

**Nel caso di comunicazioni cartacee**, ricevuta la segnalazione, il Gestore delle Segnalazioni attribuirà alla Segnalazione un codice univoco, non riconducibile alle generalità del Segnalante e protocollerà la segnalazione in particolare identificando con precisione:

- giorno e ora di ricezione;
- oggetto della segnalazione;
- stato della segnalazione (da compilare ad ogni fase del processo, ad es. istruttoria preliminare, istruttoria e comunicazione delle evidenze emerse, archiviazione).

Al ricevimento della Segnalazione, **non oltre 7 giorni dalla data di ricezione**, il Gestore delle Segnalazioni invia una comunicazione di avvenuta ricezione e presa in carico della Segnalazione. La comunicazione viene inviata attraverso il medesimo sistema utilizzato dal Segnalante, tramite modalità espressamente autorizzate dallo stesso.

La documentazione dovrà essere raccolta in un fascicolo riservato custodito dal Gestore delle Segnalazioni presso l'indirizzo in cui è domiciliato ai fini dell'espletamento dell'incarico di cui alla presente Policy. È onere del Gestore delle Segnalazioni provvedere a garantire il necessario livello di riservatezza del Segnalante e a gestire tutta la documentazione cartacea/informativa correlata alla Segnalazione pervenuta implementando idonee misure tecniche ed organizzative di sicurezza.

Nel caso di **Segnalazione pervenuta tramite telefono o colloquio riservato**, la documentazione e i verbali degli incontri/ telefonata dovranno essere raccolti in un fascicolo riservato custodito dal Gestore delle Segnalazioni (ed eventualmente, laddove richiesto dal Gestore delle Segnalazioni, dal Referente Locale laddove coinvolto). È onere del Gestore delle Segnalazioni provvedere a garantire il necessario livello di riservatezza del Segnalante e a gestire tutta la documentazione cartacea/informativa correlata alla Segnalazione pervenuta implementando idonee misure tecniche ed organizzative di sicurezza.

Sulle modalità di conservazione della documentazione, per tutto quanto non previsto all'interno della presente Policy, si fa riferimento all'art. 14 D Lgs. 24/2023.



## 4.2. Istruttoria (“Triage”)

L’istruttoria ha lo scopo di verificare la fondatezza e la tipologia della segnalazione ricevuta. A tal fine il Gestore delle Segnalazioni, effettuando uno screening preliminare, andrà a valutare nel merito l’**ammissibilità della segnalazione**, ossia:

- Accertamento preliminare della tipologia di illecito rispetto alla normativa in vigore, ai regolamenti applicabili alla Società, alle policy o procedure adottate dalla Società etc (i.e. fattispecie di reato presupposto ex Dlgs 231/01, violazioni della normativa privacy o del Regolamento GDPR, Codice Etico, procedure del sistema di gestione della sicurezza, gestione ambientale etc);
- Valutazione preliminare di ammissibilità della Segnalazione con riferimento alla qualifica soggettiva della persona Segnalante<sup>2</sup>, alla descrizione dei fatti e agli eventuali documenti e delle evidenze presentate a supporto;
- Identificazione dell’Organo Societario competente per la tipologia di violazione segnalata (i.e. Consiglio di Amministrazione, Collegio Sindacale, Organismo di Vigilanza 231/01, DPO, Datore di Lavoro prevenzionistico, Responsabile HR, etc);
- Il Gestore delle Segnalazioni valuta se richiedere ulteriori informazioni al segnalante, attraverso il medesimo canale utilizzato dal Segnalante.

A seguito dell’istruttoria, l’Gestore delle Segnalazioni redige uno specifico memorandum o verbale da cui risulti l’esito della fase di istruttoria. Il verbale viene registrato nella piattaforma MyWhistleblowing IMA o nel fascicolo riservato.

## 4.3. Indagine di merito

L’indagine di merito (o “Investigazione”) è l’insieme delle attività finalizzate a verificare il contenuto delle Segnalazioni e ad acquisire elementi utili alla successiva fase di valutazione, **garantendo in tutte le fasi la massima riservatezza sull’identità del Segnalante e sull’oggetto della Segnalazione**.

L’Indagine di merito ha lo scopo principale di verificare la veridicità delle informazioni sottoposte ad indagine, fornendo una descrizione puntuale dei fatti accertati, attraverso procedure di audit e tecniche investigative obiettive.

L’investigazione potrà essere effettuata dal Gestore delle Segnalazioni, dai singoli membri dello stesso, dai soggetti assegnatari, dai Referenti Locali, da uffici della Società espressamente incaricati dal Gestore delle Segnalazioni o da specialisti esterni ed indipendenti individuati ed incaricati dal Gestore delle Segnalazioni (“Soggetti Assegnatari”).

È compito di tutti cooperare con il soggetto incaricato dell’Investigazione nello svolgimento della stessa.

Di ogni Investigazione, il soggetto incaricato predisporrà un report finale contenente almeno:

- i fatti accertati;
- le evidenze raccolte;

<sup>2</sup> Cft art 3, comma 3 e comma 4 del Dlgs 24/2023



- le cause e le carenze che hanno permesso il verificarsi della situazione segnalata.

All'esito delle investigazioni, quando riscontri l'infondatezza della segnalazione ricevuta, il Gestore delle Segnalazioni procede all'archiviazione della segnalazione e, ove possibile<sup>3</sup>, ne informa il Segnalante.

Nel caso in cui la segnalazione risulti fondata, il Gestore delle Segnalazioni informa l'Organo identificato nel paragrafo precedente (ref. "Istruttoria/Triage") per intraprendere le azioni necessarie, definite di volta in volta in relazione alla specificità della situazione.

L'Indagine di Merito dovrà essere completata **entro 3 mesi dalla data di ricevimento della Segnalazione**<sup>4</sup>. Ad esito dell'indagine di merito il Gestore delle Segnalazioni rilascia un'informativa al Segnalante dando riscontro dell'esito dell'indagine. Il riscontro dovrà essere trasmesso al Segnalante utilizzando il medesimo canale di segnalazione impiegato per la Segnalazione ove possibile.

#### 4.4. Archiviazione

Al fine di garantire la tracciabilità, la riservatezza, la conservazione e la reperibilità dei dati durante tutto il procedimento, i documenti sono conservati e archiviati tramite la piattaforma MyWhistleblowing IMA. Qualora il Segnalante abbia utilizzato il canale verbale o la trasmissione cartacea, il Gestore delle Segnalazioni provvede a conservarla in apposito armadio messo in sicurezza presso il proprio Domicilio ed accessibile alle sole persone appositamente autorizzate ed a tale scopo istruite.

Tutta la documentazione sarà conservata, salvi gli ulteriori termini di legge nei casi espressamente previsti, per 5 anni dalla data di chiusura delle attività<sup>5</sup>, in base a quanto previsto dall'art.14 D.Lgs. 24/2023, nel rispetto degli obblighi di riservatezza.

### 5. RISERVATEZZA E TRATTAMENTO DEI DATI PERSONALI

Viene garantita la **riservatezza** dell'identità del Segnalante, secondo gli obblighi previsti dalla normativa applicabile (tra cui l'art. 12 commi 2 e ss, D. Lgs, 24/2023) durante tutte le fasi del processo e post archiviazione. Il Gestore delle Segnalazioni e tutti i soggetti ritenuti maggiormente competenti nella gestione della segnalazione eventualmente incaricati dallo stesso sono tenuti alla riservatezza dei dati personali e delle circostanze oggetto della Segnalazione.

La massima riservatezza è garantita sui soggetti e sui fatti segnalati, utilizzando, a tal fine, criteri e modalità di comunicazione idonei a tutelare l'identità e l'onorabilità delle persone menzionate nelle segnalazioni, evitando in ogni caso la comunicazione dei dati acquisiti a terzi estranei al processo di gestione delle segnalazioni.

La trasmissione e la comunicazione tra i membri dell'Gestore delle Segnalazioni e tra gli eventuali Soggetti Assegnatari è ammessa **SOLO utilizzando i canali di comunicazione**

<sup>3</sup> In relazione al canale utilizzato per la segnalazione e all'utilizzo dell'anonimato da parte del segnalante

<sup>4</sup> In conformità alla normativa applicabile ed al considerando n. 58 della Direttiva UE 2019/1937 (Cft, in particolare, art 5, comma 1, lettera d del Dlgs 24/2023)

<sup>5</sup> Cfr Art 14, comma 1 del Dlgs 24/2023



4.0

**interni alla Piattaforma MyWhistleblowing IMA.** NON è ammessa la trasmissione di documenti, informazioni, memorandum o altri dati via e-mail.

L'identità del Segnalante, secondo quanto previsto dall'art. 12 c. 2 D.Lgs. 24/2023 e dalle Leggi di Recepimento, non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle Segnalazioni, senza il consenso espresso della persona segnalante.

La gestione delle segnalazioni ed il relativo trattamento dei dati personali ivi contenuti è effettuato nel rispetto delle disposizioni di legge italiana e del Regolamento Europeo 679/2016. Nel caso di segnalazioni relative a situazioni verificatesi in Paesi diversi dall'Italia o di un segnalante non residente in Italia, la segnalazione, i dati del segnalante e la documentazione a questa associata sono comunque trattati in base alle disposizioni di legge italiane ed al Regolamento Europeo 679/2016 (GDPR)

Documenti, foto, video, registrazioni audio inviate dal segnalante che possono rappresentare una violazione di dati personali ai sensi dell'articolo 33 GDPR, della riservatezza o di altro diritto personale, o che abbiano contenuto diffamatorio e calunnioso, possono essere oggetto di provvedimenti disciplinari e/o di segnalazione alle autorità competenti.

Maggiori informazioni in merito alle modalità e alle finalità del trattamento dei dati personali raccolti in occasione delle Segnalazioni sono disponibili nell'**Allegato 1** alla presente Policy e nella pagina di accesso alla Piattaforma MyWhistleblowing IMA (esclusivamente per ciò che concerne i dati personali dei Segnalanti).

## **6. DIVIETO DI RITORSIONI E MISURE DI SOSTEGNO E PROTEZIONE DEL SEGNALANTE**

Il Segnalante **non può subire alcuna ritorsione a seguito della Segnalazione.** Il divieto di ritorsione è esteso anche ai soggetti connessi al Segnalante quali Facilitatori, familiari del Segnalante ed enti giuridici connessi al Segnalante.

Sono configurabili come ritorsioni le seguenti condotte, ai sensi dell'articolo 19 della Direttiva UE 2019/1937 e dalle relative Leggi di Recepimento di volta in volta applicabili a seconda del Paese in cui ha Società del Gruppo IMA coinvolta nella Segnalazione:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;



- i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- l’inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l’impossibilità per la persona di trovare un’occupazione nel settore o nell’industria in futuro;
- la conclusione anticipata o l’annullamento del contratto di fornitura di beni o servizi;
- l’annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

L’Autorità Giudiziaria può adottare tutte le misure, anche provvisorie, necessarie ad assicurare la tutela dei diritti del segnalante, ivi compresi il risarcimento del danno, la reintegrazione nel posto di lavoro, l’ordine di cessazione della condotta posta in essere in violazione della normativa applicabile e la dichiarazione di nullità degli atti adottati in violazione della stessa.

Conformemente a quanto previsto dalla normativa applicabile (tra cui Art. 20 del D. Lgs. n. 24/2023), è esclusa qualsiasi responsabilità penale, civile o amministrativa del segnalante che riveli o diffonda informazioni sulle violazioni

- coperte dall’obbligo di segreto (a meno che non si tratti di un obbligo di segreto imposto da norme nazionali o comunitarie in materia di informazioni classificate, segreto professionale e medico, segretezza delle deliberazioni degli organi giurisdizionali);
- relative alla tutela del diritto d’autore;
- relative alla protezione dei dati personali;
- che offendono la reputazione della persona coinvolta o denunciata;

a condizione che

- a) il segnalante, al momento della rivelazione o diffusione, avesse fondati motivi di ritenere che
  - la rivelazione o diffusione delle suddette informazioni fosse necessaria per svelare la violazione,
  - le suddette informazioni fossero vere,
  - la violazione rientrasse tra quelle previste dalla normativa applicabile e di cui al paragrafo 5 della presente Policy,
- b) la segnalazione sia stata effettuata nel rispetto delle modalità previste dalla normativa applicabile e di cui al paragrafo 5 della presente Policy.

Non è però esclusa la responsabilità penale, civile o amministrativa del Segnalante in caso di

- comportamenti, atti o omissioni non collegati alla segnalazione o che non sono strettamente necessari a rivelare la violazione;
- comportamenti posti in essere per l’acquisizione o l’accesso alle informazioni sulle violazioni previsti dalla legge come reato.

Resta ferma l’applicazione delle disposizioni in materia di esercizio del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati, di protezione contro le condotte o gli atti illeciti posti in essere in ragione di tali consultazioni, nonché di repressione delle condotte antisindacali.



Ad ogni modo, il soggetto che

- a) effettui, con dolo o colpa grave, segnalazioni che si rivelano infondate, finalizzate al solo scopo di danneggiare o recare pregiudizio a persone, processi o alla Società,
- b) effettui una segnalazione fuori dai casi e/o dalle modalità previste dalla normativa applicabile.

decade dalle misure di protezione e sostegno previste dalla normativa applicabile e può essere soggetto, a provvedimenti disciplinari, in linea con il CCNL di riferimento, oltre che alle ulteriori opportune azioni normativamente previste.

## **7. ATTIVITA' INFORMATIVA**

Ciascuna delle Società del Gruppo IMA avrà cura di condividere le più opportune informazioni sullo strumento del whistleblowing e su quanto previsto dalla presente Policy.



## **ALLEGATO 1 - INFORMATIVA AI SENSI DEGLI ART. 13-14 GDPR**

I dati personali, così come definiti dal Regolamento Generale sui Dati Personali (UE) 2016/679 (“GDPR”), che dovessero venire acquisiti in occasione di una Segnalazione ai sensi della presente Policy, saranno trattati in piena conformità a quanto ivi stabilito ed a quanto stabilito dalle altre normative vigenti in materia di protezione dei dati personali, e saranno limitati a quelli strettamente necessari per verificare la fondatezza della Segnalazione stessa e per le attività di indagine qui sopra descritte.

### **i. Titolare del trattamento**

Il titolare del trattamento dei dati personali di cui al successivo paragrafo ii) è la società del Gruppo IMA con la quale intrattiene rapporti lavorativi e/o commerciali (e.g. di cui è dipendente, tirocinante, collaboratore, cliente, fornitore, etc.) e nell’ambito della quale effettua/viene effettuata la segnalazione (“Titolare” o “Società”).

L’elenco aggiornato delle società del Gruppo IMA può essere consultato sul sito: <https://ima.it/it/il-gruppo-ima/societa-del-gruppo-ima/>.

Il Data Protection Officer nominato dalla Società è raggiungibile al seguente indirizzo mail: [dataprotectionit@ima.it](mailto:dataprotectionit@ima.it).

### **ii. Dati personali oggetto di trattamento - Interessati.**

Nell’ambito della presente Policy i dati personali oggetto di trattamento saranno i dati identificativi del Segnalante, dei segnalati, di eventuali altre persone coinvolte nella segnalazione e/o quelli afferenti i fatti segnalati e/o oggetto di indagine (ivi inclusi eventuali dati sensibili, quali l’origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l’adesione a partiti politici, sindacati, nonché i dati personali idonei a rivelare lo stato di salute e l’orientamento sessuale, o dati relativi a condanne penali o reati).

### **iii. Soggetti che gestiscono segnalazioni.**

Il trattamento dei dati personali sarà effettuato dal Gestore delle Segnalazioni (in qualità di autorizzato al trattamento dei dati), che potrà comunicare i dati personali ricevuti ai componenti dell’Organismo di Vigilanza (anch’essi in qualità di “incaricati” del trattamento) ed, a seconda dei casi, ad altri organi sociali e alle funzioni interne della Società interessata. In taluni casi, i dati personali potranno altresì essere comunicati a soggetti esterni, previo apposito incarico e con l’assunzione dei relativi obblighi di riservatezza.

I dati personali contenuti nelle Segnalazioni potranno essere comunicati anche all’Autorità Giudiziaria, ai fini dell’attivazione delle procedure necessarie a garantire, in conseguenza della Segnalazione, idonea tutela giudiziaria e/o disciplinare nei confronti del/i soggetto/i segnalato/i, laddove dagli elementi raccolti e dagli accertamenti effettuati emerge la fondatezza delle circostanze inizialmente segnalate.

Il DPO della Società vigilerà sull’esecuzione puntuale da parte del Gestore delle Segnalazioni (e degli ulteriori – eventuali - soggetti coinvolti) dei principi e regole previste dal presente protocollo in materia di protezione dei dati personali.



iv. **Finalità del trattamento - Base giuridica – Periodo di conservazione dei dati - Misure organizzative e tecniche.**

- a. **Finalità del trattamento.** Il trattamento dei dati personali sopra indicati sarà effettuato ai soli fini di dare esecuzione a quanto stabilito dal presente protocollo e, dunque, per la corretta gestione delle Segnalazioni ricevute, oltre che per l'adempimento di obblighi di legge o regolamentari nel pieno rispetto della riservatezza, dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, con particolare riferimento alle misure di sicurezza e alla tutela della riservatezza dei soggetti coinvolti e delle informazioni contenute nelle Segnalazioni.
- b. **Base giuridica.** Fermo restando quanto qui di seguito previsto, la base giuridica dei trattamenti effettuati ai sensi del presente protocollo è ravvisabile nell'articolo 6, par. 1 lett. c) ossia: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (in particolare le disposizioni di cui al D. Lgs. 24/2023): ciò vale anche per i trattamenti relativi a dati aventi ad oggetto condanne penali o reati (art. 10 del GDPR). Con riferimento ai dati "particolari" di cui all'art. 9 del GDPR, la base giuridica è rappresentata dall'art. 9, par. 2 lett. f) o let. g) del GDPR, ossia rispettivamente l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria e/o il perseguimento di un interesse pubblico (dato dalle finalità della normativa di riferimento), fermo restando che, per alcuni aspetti legati al rapporto lavorativo, la base giuridica è rinvenibile nella lett. b) della medesima disposizione (qualora chiaramente il segnalante sia un dipendente della Società).
- c. **Periodo di conservazione dei dati personali.** I dati personali trattati nell'ambito del presente protocollo saranno conservati, siano essi in formato cartaceo e/o elettronico, per un periodo di tempo di 5 anni dalla conclusione finale della procedura relativa alla gestione e/o archiviazione delle Segnalazioni.
- Resta inteso che il Titolare si riserva il diritto di conservare le Segnalazioni per un periodo più lungo laddove necessario per difendere un proprio diritto in sede giudiziale (e.g. in caso di eventuali contenziosi).
- d. **Misure tecniche ed organizzative.** Nel corso delle attività volte a verificare la fondatezza della Segnalazione saranno adottate tutte le misure necessarie a proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita e dalla divulgazione non autorizzata.
- Nell'ipotesi in cui la Segnalazione venga effettuata mediante Piattaforma, la Società informa che tale strumento è stato oggetto di valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 GDPR.
- v. **Diritti degli interessati.** La Società riconosce e tutela i diritti di tutti gli interessati i cui dati personali dovessero essere oggetto di trattamento in attuazione del presente protocollo, ai sensi degli artt. 14 – 22 del GDPR. Può esercitare i propri



diritti scrivendo una email all'indirizzo [privacy@ima.it](mailto:privacy@ima.it). Rimane per altro inteso che, in applicazione dell'art. 14, comma 5, del GDPR e dell'art. 2 *undecies* del codice privacy (D. Lgs. 196/03 e s.m.i.), la Società si riserva di non dar corso ad eventuali richieste o pretese degli interessati ove ciò possa essere di pregiudizio alla riservatezza dell'identità del Segnalante e/o rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento e possa compromettere la attività di indagine oggetto del presente protocollo.

## **ENGLISH VERSION**

### **DOCUMENT PURPOSE**

"**Whistleblowing**" is the term that identifies a report made by a person who, in carrying out his duties, becomes aware of an offence, a risk or a dangerous situation that could cause damage to the company/institution for which he works, as well as to customers, colleagues, citizens, and any other category of subjects.

IMA, sensitive to ethical issues and correct business conduct, has **implemented a system to receive and manage reports** of actions, facts or situations that may constitute unlawful conduct with respect to:

- current legislation;
- Ethical Code;
- Organization, Management and Control Model pursuant to Italian Legislative Decree no. 231/01;
- Occupational Safety Management System;
- Environmental Management System;
- as well as alleged violations of regulations and laws in the performance of work activities that could cause damage or prejudice, even if only to the image, of the Company;
- EU Regulation 679/2016 (GDPR)

The Whistleblowing Procedure adopted by IMA intends to:

- **guarantee** the confidentiality of the Whistleblower and, in the spirit of the law, protect the latter from possible retaliation;
- **promote** a culture based on responsibility and ethics;
- **allow** the corporate and control bodies of IMA to be informed of facts or conduct that is contrary to the ethical principles pursued, for the purpose of prompt intervention, as well as to identify and manage possible deficiencies in the internal control and risk management system;
- **provide** recipients with guidelines for making and managing reports effectively, “responsibly,” and in conformity with the law.

### **PROCESS RISKS**



The methodology for identifying risks and assessing the areas most exposed to the commission of 231 offenses is documented in WI\_27.2.



## TERMS AND DEFINITIONS

<b>Internal channel</b>	This means the tool adopted by IMA and by IMA Group companies subject to EU Directive 2019/1937 to allow the forwarding of reports of possible violations of laws, regulations, rules or procedures. The Internal Channel adopted by IMA and by IMA Group companies guarantees, through the application of encryption tools, the confidentiality of the identity of the Whistleblower and the related personal data, as well as the content of the Report and the related documents.
<b>DL 24/2023</b>	Means Italian Legislative Decree 10 March 2023 n. 24 <i>"Implementation of EU Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019, concerning the protection of persons who report breaches of Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions"</i> .
<b>EU Directive 2019/1937</b>	Means Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the <i>"Protection of persons who report breaches of Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions"</i>
<b>Domicile of Whistleblowing Manager</b>	Means the domicile elected by the Reporting Manager at Via Emilia, 428/442 - 40064 Ozzano dell'Emilia (BO) Italy
<b>Facilitator</b>	A person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential.
<b>IMA Group - Group</b>	Identifies IMA S.p.A. itself and all the companies controlled, directly or indirectly, by IMA S.p.A. pursuant to art. 2359 Italian Civil Code.
<b>IMA or Company</b>	IMA S.p.A. – Via Emilia, 428/442 - 40064 Ozzano dell'Emilia (BO) Italy tax code 00307140376 and VAT number 00500931209.
<b>Whistleblowing Manager</b>	It is the working group responsible for the management of Wistleblowing Reports for IMA S.p.A. and for IMA Group companies (in latter case the Reporting Manager works pursuant to art. 5 of Italian Legislative Decree 24/2023). It manages and is responsible for the correct management of the Internal Channel, the Triage phase and the Substantive Investigation. The Whistleblowing Manager is a committee made up of three independent and autonomous professionals with trasversal skills in legal and compliance matters.
<b>Implementation laws</b>	Means the national laws transposing EU Directive 2019/1937.

Each printed copy of this document, must be considered as UNCONTROLLED COPY OF WORK, the current version is available in electronic form in the intranet "QMS Factory" of the IMA Group.



<b>Reporter or Whistleblower</b>	This is the person who makes a report.
<b>Report</b>	Communication of any violation of the rules that may have an impact on the Company made according to the terms of this Policy and in compliance with the principles and rules established by Legislative Decree 24/2023.
<b>Retaliation</b>	Any conduct, act or omission, even if only attempted or threatened, committed by reason of the report or public disclosure and which causes or may cause the reporting person or the person making the report, directly or indirectly, unjust damage.
<b>Subject Reported</b>	This means the person who is the subject of the Report.
<b>MyWhistleblowing IMA</b>	<p>Web application dedicated to the management of Confidential Reports in accordance with the requirements of Italian DL 24 of 10 March 2023.</p> <p>The web application MyWhistleblowing IMA is possible to access via the website <a href="http://www.imagroup.com">www.imagroup.com</a> or the intranet MyIMA or directly to the following address:</p> <p><a href="https://areariservata.mygovernance.it/#!/WB/IMASPA">https://areariservata.mygovernance.it/#!/WB/IMASPA</a> for Whistleblowing relating to IMA S.p.A.;</p> <p><a href="https://areariservata.mygovernance.it/#!/WB/IMA-Controllate-Italia">https://areariservata.mygovernance.it/#!/WB/IMA-Controllate-Italia</a> for Whistleblowing relating to Italian companies belonging to IMA Group which are subject to the legislation;</p> <p><a href="https://areariservata.mygovernance.it/#!/WB/IMA-Europe">https://areariservata.mygovernance.it/#!/WB/IMA-Europe</a> for Whistleblowing relating to European companies belonging to IMA Group which are subject to the legislation.</p>
<b>Qualified Governance Body</b>	This means the Corporate Body, Organization or Office to which the Whistleblowing Manager reports the result of the activities carried out. It is the person responsible, by competence, for the adoption of any remedial measures or the provision of corrective actions.
<b>IMA Group Companies</b>	Means IMA S.p.A. any company controlled by it affected by the Directive EU 2019/1937.

## STANDARD REFERENCES

This Policy was drawn up with reference to the:

- **Italian Legislative Decree n. 24 of 10/3/2023** – Implementation of EU Directive 2019/1937 concerning the protection of persons who report violations of EU Law and of national regulations, and in general the Implementation Laws applicable from time to time depending on the IMA Group company involved;



- **Organization, Management and Control Model pursuant to Italian Legislative Decree 231/01** concerning the Administrative Liability of the Organisations of IMA;
- **GDPR EU 679/2016**.

For matters not explicitly dealt with in this Policy and/or for interpretation, reference is made to Italian DL 24/2023 and, where applicable, to the other implementing regulations in force in the member states in which the IMA Group companies are based.

## 1. FIELD OF APPLICATION

This Policy **applies** both in I.M.A. Industria Macchine Automatiche S.p.A and in all the companies controlled by it, directly and indirectly, and forming part of “IMA Group”, subject to EU Directive 2019/1937.

With reference to the other companies of the IMA Group based outside the European Union, IMA, as the parent company, will manage the Reports received from of the aforementioned companies, in compliance with the applicable local legislation and, to the extent compatible, in accordance with the procedures described in the present document.

Identified in this Policy are:

- the people who can activate a report;
- the acts or facts that may be the subject of a report, as well as the requirements that the reports must include in order to be taken into consideration;
- the methods for reporting the alleged violations and the people in charge of receiving the reports;
- the process of preliminary investigation and, possibly, of further investigation when a report is made;
- the protocols activated to guarantee the confidentiality of the personal data of the whistleblower and of the case in question;
- the protocols activated to guarantee the protection of the personal data of the person making the report and of the persone reported;
- the protocols activated to guarantee the prohibition of retaliation and the prohibition of discrimination against the whistleblower.

Finally, the document has the objective of ensuring that the **whistleblowing-management activities are carried out in compliance with the principles of professionalism, transparency and correctness**, in compliance with the provisions of Italian DL 24/2023 (Legislative Decree on Whistleblowing) and, more generally, with the applicable laws and regulations, as well as in compliance with the corporate Code of Ethics, the Organisation, Management and Control Model pursuant to Italian Legislative Decree 231/2001.

### 1.1. Involved subjects



The subject responsible for the management of the Internal Channel of each IMA Group Company is the **Whistleblowing Manager**, expressly appointed by each of the aforementioned Companies and authorized to carry out the activities deemed necessary for the fulfillment of the tasks assigned by Italian Legislative Decree 24/2023, by other Implementation Laws and by this Policy. The Whistleblowing Manager is a **committee** made up of three independent and autonomous professionals with trasversal skills in legal and compliance matters. For the purposes of this Policy, the committee that constitutes the Whistleblowing Manager must guarantee, in its functioning, autonomy, independence, professionalism and specific competence.

The Whistleblowing Manager may avail itself of the collaboration of internal structures of each IMA Group Company deemed more competent with respect to the case being reported.

In the event of a **conflict of interest**, i.e. those cases in which the Whistleblowing Manager coincides with the Reporter, with the reported person or is in any case a person involved or interested in the Report (this conflict may, for example, also exist with respect to the external party, in the event that the management of the platform is outsourced), the Report must be addressed to one of the members of the Management Committee of IMA S.p.A., via information sent to IMA S.p.A., Via Emilia 428/442, Ozzano dell'Emilia (BO), in sealed envelope reserved for the attention of the Management Committee in the person of the chosen member, who will take care to share its contents with the members of the Whistleblowing Manager not affected by the Report.

The right to opt to carry out the so-called "external" Report pursuant to art. 6 of Italian Legislative Decree 24/2023.

Pursuant to art. 4, sixth paragraph, of Italian Legislative Decree 24/2023, should the Report be communicated to a person other than the Whistleblowing Manager (e.g. the Supervisory Body or the Board of Statutory Auditors), the latter must forward it to Whistleblowing Manager within seven days of receipt, informing the Reporter at the same time.

The subjects **who can make a Report** are as follows ("Reporters"):

- members of the corporate bodies (Shareholders, Board of Directors, Board of Statutory Auditors, etc.);
- staff (including current employees, former employees, temporary workers, apprentices, trainees or volunteers in relation to circumstances that occurred during the employment relationship or the selection process);
- external parties who maintain relationships with IMA Group companies (i.e. stakeholders as members, customers, suppliers, agents, business associates, partners, contractors, subcontractors, as well as staff and employees of the aforementioned subjects).

## 2. REPORTING METHODS

Each IMA Group company has set up an **Internal Channel** dedicated to Whistleblowing, which can be activated via the methods described below.

### 2.1. Written form

- a) The **web application** "MyWhistleblowing IMA", reachable via the website [www.imagroup.com](http://www.imagroup.com) or the intranet MyIMA or directly to the following address:



<https://areariservata.mygovernance.it/#!/WB/IMASPA> for Whistleblowing relating to IMA S.p.A.;

<https://areariservata.mygovernance.it/#!/WB/IMA-Controllate-Italia> for Whistleblowing relating to Italian companies belonging to IMA Group;

<https://areariservata.mygovernance.it/#!/WB/IMA-Europe> for Whistleblowing relating to European companies belonging to IMA Group which are subject to the legislation..

The web application is extraneous to company servers, is managed through cloud technologies and is equipped with an encryption tool which guarantees the confidentiality of the identity of the reporting party.

The web application is permitted after user registration, and formal acknowledgment of the privacy policy and of the operating procedure.

Anonymous access is allowed.

- b) **By postal service in a sealed envelope** (registered mail) sent to the address of Whistleblowing Manager, domiciled at IMA S.p.A., Via Emilia 428/442, 40064 Ozzano dell'Emilia (BO) Italy, expressly indicating on the envelope "Whistleblowing report".

## 2.2 Oral or verbal form

Through verbal reporting on the messaging system available within the MyWhistleblowing IMA web application in which a voice and text messaging system is activated. It is also possible to request a **personal and confidential interview** with the Whistleblowing Manager. If the report concerns a company of the IMA Group with headquarters in a country other than Italy, the Whistleblowing Manager will be assisted during the interview, which will in any case remain personal and confidential, to an internal or external person of the Company involved, who speaks the native language of the Reporter ("Local Contact"). It is understood that the Local Contact must possess the characteristics of professionalism, independence and autonomy required by the applicable legislation.

Reports or information received via ordinary email, PEC, or deposited at the registered office or delivered in a manner different from the above **do not fall** under this Policy, and consequently do not benefit from the protections provided by applicable e laws.

## 2.3 External channel

As regards the IMA Group companies based in Italy, as provided for by Italian Legislative Decree no. 24 of 10 March 2023, the National Anti-Corruption Authority (ANAC) has activated an "**External**" **Whistleblowing Channel** to which the Whistleblower can make a Report if, at the time of its submission, one of the following conditions occurs:

- a) the mandatory activation of the internal Whistleblowing Channel is not foreseen within his/her work context or this, even if mandatory, is not active or, even if activated, does not comply with the provisions of article 4 of the Decree;
- b) the Whistleblower has already made a Report through the internal Whistleblowing Channel pursuant to Article 4 of the Decree and the same has not been followed up;
- c) the Whistleblower has reasonable grounds to believe that, if he/she made a Report



through the internal Whistleblowing Channel, it would not be followed up effectively or that the Report itself could lead to the risk of retaliation;

- d) the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

About IMA Group companies based in a country other than Italy, if the above conditions are met, External Reports may be made to the competent authorities designated by the member state in which the Company involved is based, pursuant to the Article 11 of EU Directive 2019/1937.

### 3. WHAT CAN BE REPORTED

It may be the subject of **internal reporting** - that is, through the whistleblowing channel that IMA has decided to adopt (see par. 2.1 and 2.2 of this Policy) – any behaviour, act or omission which harms the public interest or the integrity of IMA and/or an IMA Group company and which includes (or is reasonably believed to include):

- a) a crime, already relevant pursuant to Italian Legislative Decree n. 231/2001 (except for those companies of the IMA Group that have not adopted their own Organizational Management and Control Model pursuant to Legislative Decree no. 231/2001);
- b) a violation of the Organizational Management and Control Model adopted by IMA pursuant to Italian Legislative Decree no. 231/2001 (except for those companies of the IMA Group that have not adopted their own Organizational Management and Control Model pursuant to Legislative Decree no. 231/2001);
- c) a violation of community and national regulations regarding
  - public procurements
  - financial services, products and market abuse crimes
  - money laundering and terrorist financing
  - product safety and conformity
  - environmental protection
  - radiation protection and nuclear safety
  - food safety
  - animal health and welfare
  - public health
  - consumer protection
  - privacy and protection of personal data
  - network security and information systems
- d) a violation of laws and regulations protecting and guaranteeing the financial interests of the European Union;
- e) a violation of laws and regulations designed to protect and guarantee competition and the free circulation of goods, people, services and capital within the EU market;



- f) a practice (not non-compliant, but) in any case elusive of the community rules referred to in the previous points c), d) and e);
- g) a violation or deficiency concerning the management system for the prevention of corruption adopted by the IMA Group

In the presence of the conditions already indicated in paragraph 2.3 of this Policy, only the violations pursuant to Italian Legislative Decree no. 24/2023, i.e. those listed above in letters a) to f), can also be the subject of **external reporting** (i.e. through the whistleblowing channel set up by ANAC).

In any case, Italian Legislative Decree no. 24/2023 expressly provides that mere "irregularities", i.e. those improper behaviors which do not, however, constitute a crime or violation, cannot be reported - neither through the internal channel of IMA, nor through the external one prepared by ANAC. of the regulations listed above.

The report **must be sufficiently comprehensive**<sup>6</sup>, and rendered in great detail, with elements such as to bring out facts and situations, relating them to specific contexts and occurring in the work environment, specifying that no further personal data will be collected than that strictly necessary for the management of the Report itself and that, in the event of accidental collection, these will be immediately deleted by the Whistleblowing Manager. The Whistleblower is therefore required to provide all the available and useful elements to enable the Whistleblowing Manager to carry out the due and appropriate checks and verifications to verify the validity of the reported facts, such as, but not limited to:

- i. a clear and complete description of the facts that are the subject of the report;
- ii. the circumstances of time and place in which the facts that are the subject of the report were committed;
- iii. the particulars or other elements enabling the identification of the person(s) who has/have carried out the reported facts (i.e. job title, place of employment where he/she carries out the activity);
- iv. any documents supporting the report;
- v. any other information that may provide useful feedback on the existence of the reported facts.

The following are **not included in the scope of this Policy**:

- reports on situations of a personal nature concerning claims or grievances relating to relations with hierarchical superiors or colleagues, as well as relating to the performance of one's job;
- reports based on mere suspicions or rumours concerning personal facts that do not constitute an offence: this is because it is necessary both to take into account the interests of the third parties that are the subject of the information reported, and to avoid the Company carrying out internal inspections that risk being of little use and in any case

---

<sup>6</sup> A report can be considered detailed if it makes it possible to identify factual elements that are reasonably sufficient to start an investigation (e.g.: the offence committed, the reference period and possibly the value, causes and purpose of the offence, the company/concerned division, the persons/units involved, the anomaly in the control system).



costly.

Anonymous reports will be taken into consideration exclusively in the presence of all the elements that can allow the Whistleblowing Manager to proceed with an independent investigation; otherwise they will be archived.

## 4. MANAGEMENT OF REPORTS

Once a report is received according to the Internal channel provided in this Policy, through the written or verbal methods described in the previous paragraph, it is handled as follows:

### 4.1 Protocol and custody

If the report is made by accessing **web application MyWhistleblowing IMA**, it is the application itself that manages the protocol phase through an encryption system and issuance of a unique identification code in compliance with the reference legislation.

The encryption key is kept by the Whistleblowing Manager which may use it only and exclusively with the express and formal consent of the Whistleblower or by order of the competent Judicial Authority.

Upon receipt of the Report, **no later than 7 days from the date of receipt**, the Whistleblowing Manager, via web application, sends a communication of receipt and acceptance of the Report. The communication is sent via encrypted communication.

**In the case of paper communications**, once it has received the report the Supervisory Body will attribute a unique code to the report, not attributable to the identity of the Whistleblower, and will log the report, precisely identifying:

- date and time of receipt;
- subject of the report;
- status of the report (to be filled in at each stage of the process, i.e. preliminary investigation, investigation and communication of emerging evidence, archiving).

Upon receipt of the Report, **no later than 7 days from the date of receipt**, the Whistleblowing Manager sends a communication of receipt and acceptance of the Report. The communication is sent through the same system used by the Reporter, through methods expressly authorized by the same.

The documentation shall be collected in a confidential file kept by the Whistleblowing Manager at the address where it is domiciled for the purpose of carrying out the task referred to in this Policy. It is the duty of the Supervisory Body to ensure the necessary level of confidentiality of the Whistleblower and to manage all of the paper/electronic documentation related to the report received by implementing appropriate technical and organisational security measures.

In the case of a **Report received via telephone or confidential interview**, the documentation and minutes of the meetings/phone call must be collected in a confidential file kept by the Whistleblowing Manager (and possibly, where requested by the Whistleblowing Manager, by the Local Contact where involved). It is the responsibility of the Whistleblowing Manager to ensure the necessary level of confidentiality of the Reporter and to manage all the paper/IT



documentation related to the Report received by implementing suitable technical and organizational security measures.

On the methods of storing documentation, for anything not provided for in this policy, reference is made to art. 14 Italian Legislative Decree no. 24/2023.

## 4.2 Preliminary investigation (“Triage”)

The purpose of the investigation is to verify the validity and type of the report received. To this end, the Whistleblower Manager will evaluate the **admissibility of the report** on its merits, carrying out an initial *screening*, aimed at:

- Preliminary ascertainment of the type of offence with respect to the laws in force, the regulations applicable to the Company, the policies or procedures adopted by the Company, etc. (i.e. predicate offence cases pursuant to Legislative Decree 231/01, violations of privacy laws or the GDPR Regulation, market abuse, Code of Ethics, safety management system procedures, environmental management, etc.);
- Preliminary assessment of the admissibility of the report with reference to the subjective qualification of the Reporting person<sup>7</sup>, the description of the facts, and any supporting documents and evidence presented;
- Identification of the competent Corporate Body for the type of violation reported (i.e. Board of Directors, Board of Statutory Auditors, Supervisory Committee 231/01, DPO, Prevention Employer, HR Manager, etc.);
- The Whistleblower Manager evaluates whether to request further information from the Whistleblower, through the same channel used by the Whistleblower to submit the report.

Following the preliminary investigation, the Whistleblower Manager draws up a specific memorandum or report which shows the outcome of the investigation phase. The report is recorded on the MyWhistleblowing IMA or in the confidential file.

## 4.3 Substantive investigation

The substantive investigation (or “Investigation”) is the set of activities aimed at verifying the content of reports and acquiring useful elements for the subsequent assessment phase, **guaranteeing at all stages the utmost confidentiality on the identity of the Whistleblower and the subject of the report.**

The main purpose of the substantive investigation is to verify the veracity of the information submitted for investigation, providing an accurate description of the facts established, through audit procedures and objective investigative techniques.

The investigation may be carried out by the Whistleblower Manager, by the single members of the same, by Local Contacts, by offices of the Company expressly appointed by the Whistleblower Manager, or by external and independent specialists identified and appointed by the Supervisory Body (“Assigned Subjects”).

<sup>7</sup> Cf. art 3, paragraph 3 and paragraph 4 of Legislative Decree 24/2023



It is the duty of everyone involved to cooperate with the person in charge of the investigation in carrying out the same.

For each investigation, the person in charge will prepare a final report containing, at least:

- the established facts;
- the evidence gathered;
- the causes and deficiencies that have allowed the occurrence of the reported situation.

At the end of the investigation, in the case that it determines that the report received is without basis, the Whistleblower Manager proceeds with the archiving of the report and, where possible<sup>8</sup>, informs the Whistleblower.

In the case in which the report proves founded, the Whistleblower Manager informs the body identified in the preceding paragraph (see “Investigation / Triage”) to take the necessary actions, defined on a case-by-case basis in relation to the specificity of the situation.

The substantive investigation must be completed **within 3 months of the date the report was received**<sup>9</sup>. At the end of the substantive investigation, the Whistleblower Manager issues a report to the Whistleblower confirming the outcome of the investigation. This feedback should be sent to the Whistleblower using the same reporting channel as was used for the report.

#### 4.4 Archiving

In order to ensure traceability, confidentiality, preservation and retrievability of data throughout the proceedings, the documents are stored and archived through MyWhistleblowing IMA. If the Whistleblower has used a verbal channel or paper transmission, the Supervisory Body shall store it in a specially secured cabinet located at its Domicile and accessible only to persons specifically authorised and instructed for the purpose.

All of the documentation will be retained, subject to further legal deadlines in the cases expressly provided for, for 5 years from the date of closure of the activities<sup>10</sup>, based on the provisions of art.14 Italian Legislative Decree 24/2023, in compliance with confidentiality obligations.

### 5. PRIVACY AND PROSESSING OF PERSONAL DATA

It is guaranteed the **confidentiality** of the Whistleblower’s identity, according to the obligations established by applicable legislation (including art. 12 paragraph 2 and following Italian Legislative Decree 24/2023), during all stages of the process and post-archiving. The Whistleblower Manager and all the subjects deemed most competent in managing the report possibly appointed by the same are bound by the confidentiality of the personal data and circumstances covered by the report.

The utmost confidentiality shall be ensured with regard to the persons and facts reported, using, to this end, criteria and methods of communication suitable for protecting the identity

<sup>8</sup> In relation to the channel used for reporting and the use of anonymity by the reporting party

<sup>9</sup> In compliance with the applicable legislation and recital no. 58 of EU Directive 2019/1937(Cf.in particular art 5, paragraph 1, letter d of Legislative Decree 24/2023

<sup>10</sup> Cf. Art 15, paragraph 1 of Legislative Decree 24/2023



and reputation of the persons mentioned in the reports, avoiding in any case the communication of the data acquired to third parties extraneous to the reporting process.

Transmission and communication between members of the Whistleblower Manager and any Assigned Parties is permitted **ONLY using the internal communication channels of the MyWhistleblowing IMA**. The transmission of documents, information, memorandums or other data via e-mail is NOT permitted.

The identity of the Whistleblower, according to the provisions of the art. 12 paragraph 2 Italian Legislative Decree 24/2023 and by Implementation laws, cannot be disclosed to people other than those competent to receive or follow up on the Reports, without the express consent of the reporting person.

The management of reports and the related processing of data for privacy purposes is carried out in compliance with the provisions of Italian law and European Regulation 679/2016. In the case of reports relating to situations that occurred in countries other than Italy or by a non-resident whistleblower in Italy, the report, the data of the Whistleblower, and the associated documentation are in any case treated according to the provisions of Italian law and European Regulation 679/2016 (GDPR).

Documents, photos, videos, and audio recordings sent by the Whistleblower that may represent a violation of “privacy”, pursuant to art. 33 GDPR, confidentiality, or other personal rights, or which have defamatory or slanderous content, may be subject to disciplinary measures or reporting to the competent authorities.

Further information regarding the methods and purposes of the processing of personal data collected during the Whistleblowers is available in **Annex 1** to this Policy and on the access page to the MyWhistleblowing IMA (exclusively for what concerns the personal data of the Whistleblowers).

## **6. PROHIBITION OF RETALIATION AND SUPPORT AND PROTECTION MEASURES FOR THE WHISTLEBLOWER**

The Whistleblower **may not suffer any retaliation as a result of the report**. The prohibition of retaliation is also extended to persons connected to the Whistleblower, such as facilitators, family members of the Whistleblower and legal entities connected to the Whistleblower.

The following conduct constitutes retaliation, pursuant to article 19 of EU Directive 2019/1937 and the relevant Transposition Laws applicable from time to time depending on the country in which the IMA Group company is involved in the Report:

- dismissal, suspension or equivalent measures;
- demotion or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or unfavourable treatment;



- the non-conversion of a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- insertion in improper lists on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- early termination or cancellation of the contract for the supply of goods or services;
- cancellation of a license or permit;
- the request to undergo psychiatric or medical examinations.

The Judicial Authority may adopt all measures, even temporary, necessary to ensure the protection of the rights of the Whistleblower, including compensation for damages, reinstatement in the workplace, ordering to cease the conduct carried out in violation of the applicable law and the declaration of nullity of the acts adopted in violation of the same.

In accordance with the provisions of the applicable legislation (including art. 20 of Italian Legislative Decree no. 24/2023), any criminal, civil or administrative liability of the reporter who reveals or disseminates information on violations is excluded:

- covered by secrecy (unless it is an obligation of secrecy imposed by national or community rules on classified information, professional and medical secrecy, secrecy of judicial decisions);
- relating to the protection of copyright;
- relating to the protection of personal data;
- that offend the reputation of the person involved or reported;

provided that

- a) the reporting party, at the time of disclosure or disclosure, had reasonable grounds to believe that
  - the disclosure or dissemination of the aforementioned information was necessary to reveal the violation,
  - the above information was true,
  - the violation was among those provided for by the applicable legislation and referred to in paragraph 5 of this Policy,
- b) the report was made in compliance with the methods established by the applicable legislation and referred to in paragraph 5 of this Policy.

However, the criminal, civil or administrative liability of the Reporter is not excluded in the event of

- behaviors, acts or omissions not connected to the report or which are not strictly necessary to reveal the violation
- behaviors implemented for the acquisition or access to information on violations envisaged by law as a crime.

The application of the provisions regarding the exercise of the right of workers to consult their



representatives or unions, protection against illegal conduct or acts carried out as a result of such consultations, as well as the repression of anti-union conduct remains unchanged.

In any case, the subject that

- a) makes, with malice or gross negligence, reports that turn out to be unfounded, with the sole purpose of damaging or prejudicing persons, processes or the Company;
- b) makes a report outside the cases and/or methods provided by the applicable legislation;

may be subject to disciplinary measures, in line with the relevant CCNL (National Collective Bargaining Agreement), in addition to further appropriate regulatory actions.

## **7. INFORMATION ACTIVITY**

Each of the IMA Group companies will take care to share the most appropriate information on the whistleblowing tool and on the provisions of this Policy.



## **ANNEX 1 – INFORMATION PURSUANT ART. 13-14 GDPR**

Any personal data, as defined by the General Data Protection Regulation (EU) 2016/679 ("GDPR"), that may be acquired in connection with a Report pursuant to this Procedure shall be processed in full compliance with the provisions set forth therein and other applicable data protection regulations, and shall be limited to that which is strictly necessary to verify the merits of the Report itself and for the investigative activities described above.

### **i. Data controller**

The data controller of the personal data referred to in paragraph ii) below is the company of the IMA Group with which you have a working and/or business relationship (e.g. of which you are an employee, trainee, collaborator, customer, supplier, etc.) and within which a Report is made ("Data Controller" or "Company").

The updated list of IMA Group companies can be found at: <https://ima.it/it/il-gruppo-ima/societa-del-gruppo-ima/>.

The Data Protection Officer appointed by the Company can be reached at the following email address: [dataprotectionit@ima.it](mailto:dataprotectionit@ima.it).

### **ii. Personal Data Subject to Processing - Data Subjects.**

In the context of this Procedure, the personal data subject to processing will be the identifying data of the Reporting Party, the reported persons, any other persons involved in the reporting and/or those pertaining to the facts reported and/or under investigation (including any special categories of personal data, such as racial and ethnic origin, religious or philosophical beliefs, political opinions, membership in political parties, trade unions, as well as personal data disclosing health and sexual orientation, or data relating to criminal convictions or offenses).

### **iii. Persons handling reports.**

The processing of personal data will be carried out by the Whistleblowing Manager (as the person authorized to process the data), who may communicate the personal data received to the members of the Supervisory Board (also as "authorized personnel") and, as appropriate, to other corporate bodies and internal functions of the Company concerned. In some cases, personal data may also be disclosed to third parties, subject to a special assignment and the assumption of the relevant confidentiality obligations.

The personal data contained in the Reports may also be communicated to the Judicial Authority, for the purpose of activating the procedures necessary to guarantee, as a result of the Report, appropriate judicial and/or disciplinary protection against the person(s) reported, where from the elements collected and the investigations carried out it emerges that the circumstances initially reported are justified.

The Company's DPO will supervise the punctual execution by the Whistleblowing Manager (and the additional - if any - subjects involved) of the principles and rules provided for in this protocol regarding the protection of personal data.

### **iv. Purpose of processing - Legal basis - Period of data retention - Organizational and technical measures.**



- a. Purposes of processing.** The processing of the aforementioned personal data will be carried out solely for the purpose of implementing the provisions of this protocol and, therefore, for the proper management of the Reports received, as well as for the fulfilment of legal or regulatory obligations with full respect for confidentiality, fundamental rights and freedoms, and the dignity of the persons concerned, with particular reference to security measures and the protection of the confidentiality of the persons involved and the information contained in the Reports.
- b. Legal basis.** Without prejudice to what is set forth below, the legal basis of the processing carried out under this protocol can be found in Article 6(1)(c), i.e.: the processing is necessary to comply with a legal obligation to which the Data Controller is subject (in particular the provisions of Legislative Decree 24/2023): this also applies to processing relating to data concerning criminal convictions or offenses (Article 10 of the GDPR). With reference to the "special" data referred to in Article 9 of the GDPR, the legal basis is represented by Article 9(2)(f) or (g) of the GDPR, i.e., respectively, the establishment, exercise or defense of a right in court and/or the pursuit of a public interest (given by the purposes of the relevant legislation), it being understood that, for some aspects related to the employment relationship, the legal basis can be found in subparagraph (b) of the same provision (if clearly the reporter is an employee of the Company).
- c. Period of retention of personal data.** Personal data processed under this protocol will be retained, whether in paper and/or electronic format, for a period of time of 5 years from the final conclusion of the procedure related to the management and/or archiving of the Reports. It is understood that the Data Controller reserves the right to retain Reports for a longer period where necessary to defend its own right in court (e.g. in case of any litigation).
- d. Technical and organizational measures.** In the course of activities aimed at verifying the merits of the Report, all necessary measures will be taken to protect personal data from accidental or unlawful destruction, loss, and unauthorized disclosure.

In the event that the Reporting is made through a Platform, the Company informs that this tool has been subject to a data protection impact assessment pursuant to Article 35 GDPR.

**v. Rights of Data Subjects.**

The Company recognizes and protects the rights of all data subjects whose personal data should be processed in implementation of this Protocol, pursuant to Articles 14 - 22 of the GDPR. You may exercise your rights by writing an email to [privacy@ima.it](mailto:privacy@ima.it). It is otherwise understood that, in application of Article 14(5) of the GDPR and Article 2 *undecies* of the Privacy Code (Legislative Decree 196/03, as amended), the Company reserves the right not to give effect to any requests or claims of data subjects where this may be prejudicial to the confidentiality of the identity of the Reporting Party and/or may risk making it impossible or seriously prejudicing the achievement of the purposes of the processing and may compromise the investigative activity covered by this protocol.



## **APPROVAZIONE ELETTRONICA DEL DOCUMENTO/ ELECTRONIC APPROVAL OF THE DOCUMENT**

**Riepilogo del Flusso Approvativo del Documento (*Summary of the approval process*),  
MAN\_whistleblowing - Rev.1.7:**

**Distribuzione del / *Distribution of*: 30/04/2026**

Pratica QMS-Factory (*QMS Factory File*) N°: 2022\_1

Redatto da (*Written By*): **Renzulli Maria Pia**

Autorizzazione alla modifica/emissione (*Change/Issue Authorization*): **Fricano Beny; of 17/04/2026**

Verificato da (*Verified By*): **Monesi Iames; of 17/04/2026**

Approvato da (*Finally Approved By*): **Ferioli Massimo; of 21/04/2026**



## **STORICO REVISIONI (VERSION HISTORY)**

<b>Rev.</b>	<b>Descrizione e approvazione della modifica</b> <i>(Change description and approval)</i>	<b>Impatto della modifica</b> <i>(Change impact)</i>
1.7	The application has been extended to the Italian company ALPHAMAC Srl. Updated new website address.	<b>Medium:</b> the web application <i>MyWhistleblowing IMA</i> address is published both on website <a href="http://www.imagroup.com">www.imagroup.com</a> and on MyIMA intranet. The tutorial for use can be found in web application itself.
1.6	The application has been extended to the Italian company Perfect Pak Srl and Spares Service & Machinery Srl. FASP Srl was cancelled.	<b>Medium:</b> the web application <i>MyWhistleblowing IMA</i> address is published both on website <a href="http://www.ima.it">www.ima.it</a> and on MyIMA intranet. The tutorial for use can be found in web application itself.
1.5	The application has been extended to the Italian company Record SpA.	<b>Medium:</b> the web application <i>MyWhistleblowing IMA</i> address is published both on website <a href="http://www.ima.it">www.ima.it</a> and on MyIMA intranet. The tutorial for use can be found in web application itself.
1.4	The application has been extended to the recently acquired Italian companies OMAS Tecnosistemi SpA and IMA Sarong Srl.	<b>Medium:</b> the web application <i>MyWhistleblowing IMA</i> address is published both on website <a href="http://www.ima.it">www.ima.it</a> and on MyIMA intranet. The tutorial for use can be found in web application itself.
1.3	The application has been extended to all the European companies controlled by IMA S.p.A., directly and indirectly, subject to EU Directive 2019/1937. Reference has been made to the management of reports concerning companies belonging to the European Non-Union IMA Group.	<b>Medium:</b> the web application <i>MyWhistleblowing IMA</i> address is published both on website <a href="http://www.ima.it">www.ima.it</a> and on MyIMA intranet. The tutorial for use can be found in web application itself.
1.2	Updated to comply with Italian Legislative Decree no. 24/2023 concerning the protection of persons who report breaches of Union law and national regulatory provisions. The application is extended to all the Italian companies controlled by IMA S.p.A., directly and indirectly, subject to EU Directive 2019/1937.	<b>Medium:</b> the new web application <i>MyWhistleblowing IMA</i> address is published both on website <a href="http://www.ima.it">www.ima.it</a> and on MyIMA intranet. The tutorial for use can be found in web application itself.
1.1	Updated to comply with UE Directive no. 1937/2019 about Whistleblowing	<b>Medium:</b> guaranteed confidentiality about the identity of the whistleblower and the processing of data in compliance with the GDPR. Training is not required.
1.0	First issue: Italian Law no.179 of 30 November 2017 compliant	High impact on the process owner, HR Dir.. For this reason, training is not needed

Each printed copy of this document, must be considered as UNCONTROLLED COPY OF WORK, the current version is available in electronic form in the intranet "QMS Factory" of the IMA Group.