



# **IBA Group Policy**

## **Whistleblower Process**

**Effective Date: 20 April 2026**





**Approved by: CEO, CFO, CLO, Works Council (consultation)**  
**Last update : 20 April 2026**  
**Version : 1.0**





## Contents

INTRODUCTION AND DEFINITIONS.....	4
Introduction.....	4
Definitions .....	4
COMPLIANCE REPORTING FRAMEWORK.....	5
What can be reported? .....	5
Who can report? .....	5
Where to report.....	5
RULES APPLICABLE TO REPORTING.....	6
Submitting a report.....	6
Confidentiality and data protection.....	6
No retaliation against employees.....	7
RULES APPLICABLE TO THE INVESTIGATIONS.....	7
General principles .....	7
Investigation process .....	7
RECORD KEEPING, RETENTION AND DISCLOSURE.....	8
ENTRY INTO FORCE AND REVISION.....	8





## INTRODUCTION AND DEFINITIONS

### Introduction

This Policy describes how concerns about breaches of IBA's Code of Business Conduct or of applicable law related to the twelve Principles described in the Code of Business Conduct can be reported and handled within the Company and the Group through protected internal channels. It applies to all employees and other people who obtain information in a work-related context, such as temporary workers, contractors & consultants, suppliers, shareholders, members of management, trainees and volunteers. If you have any questions or are in any doubt as to how to comply with this Policy, please speak to the Company's Chief Legal Officer (the **Compliance Officer**) (e-mail: [LegalCompliance@iba-group.com](mailto:LegalCompliance@iba-group.com)). The Compliance Officer has been appointed by Management to supervise compliance with Applicable Laws and regulations, the IBA Code of Business Conduct and this Agent Commission Policy.

While other external reporting channels are available (such as mentioned under "Applicable Laws"), any irregularities or suspected non-compliance should preferably be notified through the Whistleblower Platform, SpeakUp, on IBA's official website (<https://www.iba-worldwide.com/iba-code-conduct>).

The Policy will be published on the Company website, the Company intranet and the Legal SharePoint. Regular communications and reminders will be sent out to all employees to ensure awareness.

### Definitions

**Applicable Law(s)** means, without limitation, the Belgian Whistleblowers Act for the private sector, dated 28 November 2022 which entered into force on 15 February 2023 and transposes EU Directive 2019/1937 on the protection of persons who report breaches of Union law. Applicable Law further includes applicable data protection legislation, including the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), and the Belgian labor and privacy rules embedded in the DPA Act of 3 December 2017 and the Framework Act of 30 July 2018. Applicable Law will also include any executive orders with respect to the abovementioned laws, such as the Belgian Royal Decree dated 22 January 2023 clarifying article 14 of the Whistleblower Law relating to the possible 24 external notification channels.

**Company** means Ion Beam Applications SA, or in abbreviated form, IBA SA, or IBA.

**IBA Code of Business Conduct (or the Code)** means the Company's Code of Business Conduct and the Company's Suppliers Code where applicable, as published on the Company's website from time to time.

**Group** means Ion Beam Applications SA and its subsidiaries.



**Investigator** means the individual or individuals appointed by the Company to investigate a report on a suspected breach of the Code or the law, in respect of Applicable Laws. In the IBA context, this is the Compliance Officer. The Compliance Officer can delegate the investigation to a Manager, a HR Manager, a Person of Trust, a member of the Company Legal team, a certified external law firm or a certified external audit or investigation firm, but always under his/her final responsibility.

**Manager** means

- (i) any member of the Leadership Teams, as defined on the Company's intranet from time to time; and
- (ii) any other employee/consultant having the authority to negotiate, decide, or overrule decisions taken by other employees, always in compliance with the Company's Delegation of Authority as applicable from time to time.

**Whistleblower Platform** means the anonymous reporting platform licensed from SpeakUp, certified to be fully compliant with applicable laws and regulation in matters of ethics and compliance, and accessible by anyone through IBA's official website (<https://www.iba-worldwide.com/iba-code-conduct>).

**Whistleblower Process** means the present IBA Group policy defining the framework in which concerns about breaches of the IBA Code of Business Conduct can be reported.

## COMPLIANCE REPORTING FRAMEWORK

### What can be reported?

Reports can relate to actual or suspected breaches of the Code of Business Conduct or applicable law related to the twelve Principles described in the Code. Because it is not always straightforward to link a specific factual situation to one of the twelve Principles of the Code or to a legal concept, the question "what can be reported" should be interpreted in the broadest possible sense.

The following are obvious areas of what facts or suspicions can be reported but they are in no way meant to be limitative: (i) fraud, bribery and corruption (financial, in kind, internal, agents, distributors) ; (ii) employee wellbeing (harassment, bullying, discrimination) ; (iii) healthcare compliance ; (iv) Company assets theft (IP, IT); (v) data protection; and (vi) financial offences.

### Who can report?

Starting from IBA's stakeholder approach and respect for its employees, customers and patients, suppliers, shareholders, society and our planet, the Company has taken the broadest possible stand with respect to who can report actual or suspected breaches of the Code of Business Conduct or applicable law. Hence, all employees of the Group and other people who obtain information in a work-related context, such as temporary workers, contractors & consultants, suppliers, shareholders, members of management, trainees and volunteers can report a concern.



## Where to report ?

A suspected breach or a concern with respect to any of the twelve Principles of the Code can be reported by anyone through the Whistleblower Platform. In most cases of concern, this is the preferred route of reporting. It is important to note that reporting through the Whistleblower Platform is fully anonymous. Alternative reporting possibilities are : the reporting channels outside of IBA, the Manager of the employee wishing to report a concern (unless the Manager is conflicted) , or the Compliance Officer (email: [LegalCompliance@iba-group.com](mailto:LegalCompliance@iba-group.com)), or the HR Manager (or “Person of Trust”). While concerns with respect to the work environment (such as bullying, harassment, discrimination, etc.) can be reported through all channels, the Company believes that they can be handled most efficiently through the Manager and/or the HR Manager or Person of Trust. Anonymity in these sorts of concerns hinders the investigation rather than resolving it.

## RULES APPLICABLE TO REPORTING

### Submitting a report

In order to ensure that the follow-up of the reporting of a concern or suspected breach of the Code or the law is as efficient as possible, employees and others are encouraged to submit a written report with as many factual details and supporting documents as possible. Reports should preferably be in writing, but verbal reports will not be refused. Providing evidence of the alleged breach of the Code or the law is not a prerequisite for the validity of the reporting.

All reporting must be made in good faith and the Investigator will always assume the presence of good faith unless otherwise proven.

### Confidentiality and data protection

The identity of the reporter (who chose to waive his/her anonymity), any person concerned and any third party mentioned in the report is kept strictly confidential and is only disclosed to individuals who need this information to handle the report or when required by law. All personal data are processed in line with Applicable Laws, including specifically GDPR, based on appropriate legal grounds, with limited access, adequate security measures, and retention only as long as necessary to manage the report and meet legal retention periods.



## No retaliation against employees

Any form of retaliation or attempted retaliation against an employee who makes a report in accordance with the Code or with the law (or assists such a person) is strictly prohibited. Retaliation includes, for example, dismissal, demotion, negative performance evaluation, changes in duties, harassment, intimidation, or adverse treatment of a similar nature, and may lead to disciplinary measures.

Protection applies where the reporter acted in good faith and had reasonable grounds to believe that the information reported was true at the time and that it fell within the scope of the Code and/or the law, even if subsequent investigations do not confirm the suspicion.

Knowingly false reports or reports made by an employee in bad faith may result in disciplinary action and do not benefit from whistleblower protection. For example, falsification of evidence and denunciation for personal reasons are considered bad faith.

## RULES APPLICABLE TO THE INVESTIGATIONS

### General principles

All reports of suspected breach of the Code or of the law will be investigated, in full respect of Applicable Law, and within a reasonable period of time.

Individuals who are the subject of a report of a suspected breach of the Code or the law will be informed by the Investigator of the existence of the report, the investigation and of their rights as soon as this can occur without jeopardizing the investigation. They must be treated fairly, be able to present their observations, and may exercise their data protection rights in accordance with Applicable Law, subject to legitimate restrictions to protect the investigation and others' rights.

All reported concerns or breaches of applicable criminal law will be notified and handed over to the competent authorities if imposed by applicable law or in the interest of the Company.

### Investigation process

Upon receipt of a report on the Whistleblower Platform, the system will automatically send a written acknowledgment of receipt. In all other reporting cases, the individual receiving the report will send an acknowledgment of receipt within 2 working days, unless the reporter explicitly requested otherwise or acknowledgment would compromise confidentiality.

Reports introduced through the Whistleblower Platform will be handled by the Compliance Officer. However, depending on the nature of the concern reported, the Compliance Officer can decide to mandate a Manager, HR Manager, Person of Trust, or certified external law firm or certified external audit or investigation firm as Investigator, but always under his/her final responsibility.

For reports not introduced through the Whistleblower Platform with respect to employee-related HR matters (such as bullying, harassment, discrimination, etc.), the Investigator will be the HR



Manager and/or Person of Trust, unless the Investigator has a conflict of interest. In the latter case, the Compliance Officer will appoint an Investigator with appropriate expertise on the subject matter.

The Investigator will conduct the investigation in an impartial way and according to a process that the Investigator sees best fit for the reported concern, which may include document review, interviews and consultation of experts, always respecting the presumption of innocence and the rights of persons concerned.

The Investigator provides feedback and if possible, the final outcome of the investigation process to the reporter within 2 months from the acknowledgment, indicating what follow up has been or will be given (for example, investigation steps or corrective measures), while protecting confidentiality and legal interests of those concerned by the investigation.

## RECORD KEEPING, RETENTION AND DISCLOSURE

All reports received through the internal channel are recorded in a secure electronic register accessible only to the Investigator, the Compliance Officer and the people referred to in the investigation final report. The register documents, the date of receipt, the channel used, the status of the report, key steps in the investigation and the outcome, while respecting confidentiality and data minimization; these records are retained only for the necessary period and then anonymized or deleted.

The Compliance Officer provides an annual written report of the activities falling within the scope of the present Whistleblower Policy to Management and the Audit & Risks Board Committee of the Company. The report will contain an overview of the cases handled (anonymizing the personal data), together with the actions taken and remediation plans, including possible changes to the present Whistleblower Policy.

## ENTRY INTO FORCE AND REVISION

This Whistleblower Policy has as effective date 20 April 2026. It can be reviewed on the recommendation of the Company Audit & Risks Board Committee, the Company Works Council, Management or the Compliance Officer. Any revision of this Whistleblower Policy requires prior consultation of the Company Works Council.

Whistleblower Policy version 1.0 dated 20 April 2026 - Signed





*Christian Matton*

---

Christian Matton  
Chief Legal Officer & Compliance Officer

*C V*

---

Catherine Vandendorre  
Chief Financial Officer, Head of Corporate

*Olivier Legrain*

---

Olivier Legrain  
Chief Executive Officer

