Policy

Whistleblowing

Septembre 2025

iKanbi

Introduction

iKanbi Group SA et ses filiales, are committed to conducting business in a fair, honest, and transparent manner while complying with all legal and regulatory obligations.

Despite our efforts to uphold this commitment, certain inappropriate behaviors or unlawful situations cannot be entirely ruled out. A culture of openness and accountability is essential to prevent such situations from occurring and to address them effectively when they do arise.

Through the whistleblowing platform, available at https://whistleblowersoftware.com/secure/ikanbi, our Group enables you to report potential violations of legislation.

Legislation in this area provides that, in the event of suspected violations, employees should first refer the matter to their direct supervisor and, failing that, use the internal reporting channel before resorting to external channels managed by the authorities.

In this way, swift and effective measures can be taken to address the situation while avoiding unnecessary pressure on public authority channels. iKanbi and its subsidiaries therefore strongly encourage whistleblowers to contact their direct supervisor or use the internal reporting channel and commit to diligent, efficient, and legally compliant follow-up.

This policy aims to inform you in particular about how the platform works, how alerts will be handled, what data is collected in this context, and the protection granted to whistleblowers under the conditions set by law.

Contents

1. Définitions

iKanbi : refers to the following companies:

iKanbi Belgium SA with its registered office at 4000 Liège, Quai Banning 6, and registered with the Belgian Crossroads Bank for Enterprises under company number 0445.248.212;

iKanbi Group SA with its registered office at 1050 Brussels, Place du Champ de Mars 5, and registered with the Belgian Crossroads Bank for Enterprises under company number 0460.263.515;

iZuwi Europe SA with its registered office at 4000 Liège, Quai Banning 6, and registered with the Belgian Crossroads Bank for Enterprises under company number 0521.718.260.

Employee or Worker: any natural person bound by an employment contract with an **iKanbi** company, within the meaning of Article 45, paragraph 1, of the Treaty on the Functioning of the European Union.

Whistleblower: any person who reports information on violations (as referred to in section 3) and who falls within the scope of the Whistleblower Protection Act or within the scope of section 2.1, whether or not that person is employed by **iKanbi**.

Facilitator: a natural person who assists a Whistleblower during the reporting process, whose assistance must remain confidential.

Third Parties: individuals who are neither Whistleblowers nor Facilitators but who are connected to the Whistleblower and risk facing retaliation in a professional context, such as colleagues or relatives of the Whistleblower.

Group: iKanbi and all companies or legal entities controlled by **iKanbi** (subsidiaries), or any company or legal entity that controls **iKanbi** (parent company), or any company or legal entity that is also controlled by the parent company (sister companies). The term control shall be understood as defined in Article 1:14 of the Belgian Code of Companies and Associations.

Violations : means any act, fact, or omission that:

- (a) is unlawful and relates to the areas falling within the material scope or the acts mentioned in section 2;
- (b) is contrary to the purpose or objective of the rules provided for in the areas falling within the material scope or the rules provided for in the acts mentioned in section 2.2.

Information on Violations: information, including reasonable suspicions, regarding actual or potential Violations that have occurred or are very likely to occur, as well as attempts to conceal such Violations.

Whistleblower Protection Act: : the Belgian law of 28 November 2022 on the protection of persons who report breaches of Union law or national law identified within a private sector legal entity, partially transposing the European Directive 2019/1937.

Whistleblower Directive : European Directive 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law.

HR Manager: the Human Resources Manager of iKanbi Belgium SA (hereinafter referred to as the "HR Manager"; the use of the neutral masculine term is without prejudice to the possibility of this role being exercised by a woman or a man).

Compliance Committee the committee responsible for receiving and handling alerts, composed of:

- the HR Manager of **iKanbi Belgium SA;**
- the Administrator (Legal, Finance, and GDPR) of **iKanbi Belgium SA;**
- the Chief Operating Officer (COO) of **iKanbi Belgium SA.**

Fieldfisher : the English law firm Fieldfisher (Belgium) LLP.

2. Scope of Application

iKanbi has established a reporting and follow-up channel that can be used through an online portal provided by the Danish company Whistleblower Software ApS, with its registered office at Kannikegade 4, 8000 Aarhus C, Denmark (the "Whistleblowing Channel").

This Whistleblowing Policy defines the conditions under which this Whistleblowing Channel may be used within iKanbi.

2.1 Personal Scope

This Whistleblowing Policy applies to individuals who have obtained information on Violations in a professional context with iKanbi, including:

- current employees or those whose employment relationship has ended;
- job applicants;
- paid and unpaid interns and trainees;
- consultants and independent service providers;
- temporary workers;
- volunteers;
- shareholders, directors, and any other person belonging to iKanbi's administrative, management, or supervisory body, including non-executive members, whether or not they are remunerated.

The Whistleblowing Channel established by iKanbi is accessible for any alert containing Information on Violations obtained by the above-mentioned persons in a professional context.

2.2. Material Scope

The Whistleblowing Channel may be used to report any Information on Violations that fall within the scope of the Whistleblower Protection Act.

The Information on Violations must relate to the following areas, in accordance with the applicable Whistleblower Protection Act:

(i) any breach of legislation in the following areas:

- public procurement;
- financial services, products and markets, and the prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- environmental protection;
- radiation protection and nuclear safety;
- food and feed safety, animal health and welfare;
- public health;
- consumer protection;
- protection of privacy and personal data, and security of networks and information systems;
- combating tax fraud;
- combating social fraud.

(ii) any breach affecting the financial interests of the European Union, as referred to in Article 325 of the Treaty on the Functioning of the European Union and specified in the relevant implementing provisions of Community or national law;

(iii) any breach relating to the internal market of the European Union as an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured, including breaches of EU competition rules and rules on State aid.

Information on Violations that does not fall within any of the above-mentioned areas cannot be reported via the internal channel described in this Policy. For example, alerts concerning possible breaches of legislation on psychosocial well-being within iKanbi (violence, moral or sexual harassment, and psychosocial aspects at work) or any other matter specifically regulated in Belgium and covered by the work regulations or any other applicable policy, must be reported through the designated procedures applicable to those issues.

For certain areas falling outside these scopes, other reporting channels exist (see section 6 “External Alerts”).

3. Alerts

3.1 Internal Whistleblowing Channel

The Whistleblowing Channel provides a unique and direct means open to all Whistleblowers for the collection and handling of internal reports containing Information on Violations, in accordance with section 2.

This portal is accessible via the following link: https://whistleblowersoftware.com/secure/ikanbi

In the event of a technical issue with the platform, Whistleblowers are invited to contact the HR Manager directly via email at whistleblowing@ikanbi.com.

Internal alerts may be submitted through the Whistleblowing Channel either in writing or orally.

An alert may also be made by personally meeting with the HR Manager or any other member of the Compliance Committee, upon the express request of the Whistleblower submitted via the online portal or by email to whistleblowing@ikanbi.com. Such a meeting (either in person or by video conference) is organized within a reasonable timeframe following the request, within two weeks of the request or, in exceptional circumstances, within one month at the latest.

If the alert is made during a video conference or a physical meeting, the conversation is recorded with the Whistleblower's consent, or alternatively, a precise written summary of the conversation is drafted. The Whistleblower verifies the content of the written summary, amends it if necessary, and signs it.

Access to information transmitted via the Whistleblowing Channel is strictly limited to:

- the HR Manager;
- other members of the Compliance Committee;
- the Managing Director of iKanbi Belgium SA (see section 3.3(i));
- members of Whistleblowing Software, who may be exposed to such information as part of their mission of maintaining the IT platform and protecting the data stored therein;
- members of the law firm Fieldfisher.

3.2 Confidentiality and Anonymity

A Whistleblower may choose to submit a report anonymously or to provide personal contact details, which will be handled with the utmost confidentiality.

If a Whistleblower decides to disclose their identity when submitting a report that falls within the scope of the Whistleblower Protection Act, the individuals listed in section 3.1 who have access to the identity-related information contained in the report will preserve the confidentiality of the Whistleblower's identity in accordance with applicable law.

As such, the Whistleblower's identity will, in principle, only be disclosed if the Whistleblower expressly and freely consents to such disclosure.

However, the Whistleblower's identity may be disclosed to public authorities, such as the police or the prosecutor's office, where this is a necessary and proportionate obligation under special legislation in the context of investigations conducted by national authorities or judicial proceedings, in particular to safeguard the rights of defense of the person concerned.

In such cases, the Whistleblower will be informed before such disclosure takes place, unless providing such information would jeopardize ongoing investigations or judicial proceedings. The HR Manager or another member of the Compliance Committee will send the Whistleblower a written explanation of the reasons for the disclosure of their confidential data.

If the Whistleblower chooses to make a report anonymously but provides information that enables iKanbi to identify them, iKanbi will be entitled to process this data.

If a Whistleblower submits a report anonymously, they will have the option to request updates on the investigation via a secure and anonymous link through which iKanbi can contact them.

The Whistleblowing Channel allows the Whistleblower to prevent the recording of their IP address or login credentials and does not use cookies.

If the Whistleblower's computer belongs to iKanbi or is connected to the iKanbi network, there is a risk that the Whistleblower's IP address and/or login credentials may be recorded in the server history through backups stored in iKanbi's IT systems. The Whistleblower can avoid this risk by submitting the report from a computer that does not belong to iKanbi and is not connected to the iKanbi network.

It is recommended that reports be made on a non-anonymous basis, as anonymity may make it more difficult to conduct an appropriate investigation and to implement adequate protection measures.

3.3 Processing of Alerts

i. Roles and Responsibilities

HR Manager: The HR Manager, assisted by the Compliance Committee, is the designated single point of contact within iKanbi for handling submitted reports. The HR Manager is supported by a team of lawyers from the Fieldfisher law firm.

The Whistleblower may indicate in their report if the HR Manager or another member of the Compliance Committee is personally involved in the reported Violation. In such a case, the report will not be forwarded to the implicated member, and the identity of the Whistleblower, any Facilitator, or Third Party will not be disclosed to that member.

Fieldfisher acts as legal advisor in the sole interest of iKanbi in accordance with the contract binding Fieldfisher to iKanbi Belgium, and in compliance with the applicable ethical rules governing its members. It is understood that all information and/or documents provided by the Whistleblower may be used by Fieldfisher (Belgium) LLP to protect iKanbi's interests as if such information and documents had been transmitted directly by iKanbi.

The designated members of the Fieldfisher law firm are responsible for receiving and forwarding to the HR Manager and the Compliance Committee all alerts and requests submitted through the Whistleblowing Channel.

If the Whistleblower indicates in their report that all members of the Compliance Committee are involved in the reported Violation and should therefore not have access to the report or to the Whistleblower's identity, Fieldfisher will in such case forward the content of the report, including the Whistleblower's identity where applicable, to the Managing Director of **iKanbi Belgium SA.**

Reports will generally be processed within three months from the acknowledgment of receipt. Within the same three-month period, feedback will be provided to the Whistleblower, informing them of the actions planned or taken in response to their report and the reasons for such actions.

ii. Initial Assessment of Reports

The HR Manager or any other member of the Compliance Committee, assisted by Fieldfisher (Belgium) LLP, will carry out an initial confidential assessment of each report in order to determine whether it falls within the scope of the Whistleblower Protection Act before a full investigation is undertaken.

If the initial assessment shows that the report does not fall within the scope of the Whistleblower Protection Act, the report will no longer be processed and the Whistleblower will be informed accordingly.

Anonymous reports will be processed if it appears from sufficiently detailed factual information that the reported Violation is credible.

iii. Investigation Following a Report

Once the initial assessment has been completed, the HR Manager or any other member of the Compliance Committee will investigate the facts indicated in the report. They may call upon any member of iKanbi's management team or any third party, as appropriate, without disclosing the identity of the Whistleblower, any Facilitators, or Third Parties to persons other than those authorized under section 3.1.

The Whistleblowing Channel is intended to ensure that any measures taken by persons responsible for receiving and/or processing a report remain confidential and that the rights of all parties are respected. Indeed, all persons authorized to access reports under section 3.1 undertake to respect their duty of confidentiality, not to use the data and information for purposes other than processing reports, not to retain them beyond the retention period, and to destroy or return them as provided for in this Policy.

3.4 Information of Persons Involved in a Report

Any person directly or indirectly involved in a report deemed to warrant further investigation will be informed by the HR Manager as soon as possible, in compliance with the applicable legal provisions and iKanbi's personal data protection policy in particular, Article 14 of the General Data Protection Regulation (GDPR).

However, if after the initial assessment the HR Manager or any member of the Compliance Committee decides to close the procedure due to lack of evidence or for other reasons, or in the case of repeated alerts that do not contain any new significant information, they may decide not to inform the persons involved in the report.

If there is a serious risk that notification of the report would compromise the investigation of the reported Violation or the possibility of obtaining necessary evidence, notification may be postponed or withheld until such risk no longer exists.

If the report contains data on other identifiable individuals in addition to the person subject to the reported Violation, those individuals will be informed as described above. This information must not include any identifiable data about other individuals concerned or about the Whistleblower.

4. Protection of Whistleblowers

Reports must be made in good faith. In particular, the Whistleblowing Channel must not be used to raise issues that the Whistleblower knows to be false.

Whistleblowers will be protected against any form of retaliation, such as sanctions or discrimination, if they have used the Whistleblowing Channel in good faith regardless of whether the subsequent investigation reveals a violation and/or an offense, whether the reported facts prove to be inaccurate or incorrect, or whether the information was initially disseminated in bad faith by someone other than the Whistleblower, who nonetheless reported it in good faith.

The same protection applies to the Whistleblower, the Facilitator, and Third Parties connected to the Whistleblower who might be subject to retaliation in a professional context, including the Whistleblower's family members.

If a person who has used the Whistleblowing Channel in good faith believes they have been subjected to retaliation, sanctions, or discrimination, they must immediately inform the HR Manager or any other manager or supervisor they consider more appropriate.

5. Secure Storage of Data

Access to data relating to reports and investigations will be restricted. If the data is stored in an iKanbi information system or in an external system, it will be protected by individual usernames and passwords, which will be changed regularly. Access will be logged and monitored.

If the data is processed outside such a system, all copies, whether digital (USB drives, etc.) or paper, will be kept securely under lock and key. The secure storage system, where data relating to reports will be retained, will ensure that no one other than the persons authorized to collect and process the reports will have access to this data.

6. External Alerts

A Whistleblower may also raise concerns through an external reporting channel, i.e., a whistleblowing channel established by an external authority.

Reporting an issue through an external channel is not conditional upon having first used the Whistleblowing Channel established by iKanbi.

However, it is recommended that reports be submitted first through iKanbi's Whistleblowing Channel so that the company can ensure prompt and immediate follow-up of the reported Violations.

External reporting is possible to the Federal Ombudsmen as provided for by the Belgian law of 22 March 1995 establishing federal ombudsmen, who are responsible for coordinating external reports in the private sector (https://www.mediateurfederal.be), or to any other person designated under Article 14 of the aforementioned Belgian law of 28 November 2022.

7. Publication

iKanbi is committed to disseminating this Policy in order to provide clear information to potential users. This Policy will be made accessible to all individuals falling within its scope, as defined in section 2.

Privacy Statement

Applicable to Whistleblowing Reports ('Statement')

Septembre 2025

iKanbi

Last updated: 09/2025

1. About this Statement

1.1 This Statement describes how we (as defined below) collect, share, and use any information that, alone or in combination with other information, relates to you ("Personal Data") when we receive and process whistleblowing reports.

1.2 In this context, we may process Personal Data relating to whistleblowers (whether employees, workers, interns, job applicants, suppliers, shareholders, etc.), persons who may be implicated by a report, facilitators who assisted the whistleblower, any witnesses and individuals interviewed as part of the verifications, and the persons handling the reports ("you" and "your").

1.3 This Statement sets out the rights you have in relation to the Personal Data we process about you, as well as how you can exercise them.

1.4 iKanbi Belgium SA, with its registered office at 4000 Liège, Quai Banning 6, and registered with the Belgian Crossroads Bank for Enterprises under company number 0445.248.212, has implemented and manages an internal channel for reporting alerts. For this purpose, it acts as the controller of your Personal Data ("iKanbi Belgium," "we," and "our"). As controller, iKanbi Belgium is responsible for ensuring that the processing of Personal Data complies with applicable data protection legislation, and in particular the General Data Protection Regulation ("GDPR"). The data subject will be informed if another entity of the iKanbi group processes personal data in the context of managing the internal reporting channel, whether that entity acts as a sole controller or processes such data jointly with iKanbi Belgium. In the latter case, the data subject may contact any of the joint controllers, although for ease of processing it is recommended to contact by default the controller designated within iKanbi Belgium.

1.5 We take our privacy obligations very seriously. This is why we have developed this Statement, which applies alongside other applicable notices, statements, or policies.

1.6 Please take the time to read this Statement carefully. If you have any questions or comments, please contact dpo@ikanbi.com.

2. What Personal Data is Collected by iKanbi Belgium and Why?

2.1 The categories of Personal Data we collect about you, and the reasons why we process them, are as follows:

Why We Process This Data	Categories of Personal Data	Legal Ground
To collect, process, and verify alerts and reports concerning misconduct. To determine and take the necessary measures following alerts.	• Identity, role, and contact details of the whistleblower (unless the whistleblower chooses to remain anonymous), of any person involved in the report, or of those handling the report. • Content of the report (including transmitted files) and data relating to the report. • Information collected during the verification of the reported behaviors. • Report on the verification process. • Follow-up actions taken in response to the report.	• Legal obligation where there is a requirement to establish an internal reporting channel. • If an internal reporting channel is set up voluntarily where it is not legally required: iKanbi Belgium's legitimate interest in enabling the reporting of certain behaviors.

2.2 If we ask you to provide any other Personal Data not described above, the Personal Data we ask you to provide, and the reasons why we ask you to provide it, will be clearly explained to you at the time of collection.

2.3 The reports we receive may contain information relating to ethnic origin, political opinions or religious beliefs, health or physical/mental condition, sexual orientation, trade union membership, or the commission (alleged or otherwise) of criminal offenses and related security measures ("Sensitive Personal Data"). Although we aim to minimize the amount of Sensitive Personal Data we process, we may process such Sensitive Personal Data in certain circumstances if permitted under applicable law, in particular where such data is necessary for the establishment, exercise, or defense of legal claims, or for fulfilling our obligations and rights in the field of employment law.

3. Who Do We Share Your Personal Data With?

3.1 As a rule, iKanbi Belgium does not disclose to third parties the Personal Data collected through the whistleblowing channel. Only duly authorized members of our staff, who are competent to access and handle alerts, will process this Personal Data.

3.2 The identity of the whistleblower, facilitators, and other third parties who may be at risk of retaliation will not be disclosed outside of the personnel authorized to receive and handle alerts, except where (1) the whistleblower has given explicit consent, or (2) disclosure is required as a necessary and proportionate obligation under specific legislation, such as in the context of investigations conducted by national authorities or judicial proceedings, particularly in order to safeguard the rights of defense of the person concerned.

3.3 However, subject to our strict confidentiality obligations, including those set out in section 3.2, we may share your Personal Data, on a case-by-case basis, with the following categories of recipients:

- (a) Group companies, only to the extent necessary for handling the alert;
- (b) Our third-party service provider (Whistleblower Software ApS), which provides the technical platform for the internal reporting channel. We require this processor to act only in accordance with our instructions and to take appropriate measures to ensure that Personal Data remains protected;
- (c) Any competent authority, including regulators, government agencies, courts, public prosecutors, police, or other third parties, where disclosure is necessary (i) under applicable laws or regulations, (ii) to exercise, establish, or defend our legal rights, including in the context of potential judicial proceedings, or (iii) to protect your vital interests or those of another person.

- (d) to our auditors and external advisors in connection with the advisory services they provide to us (e.g., for the purpose of conducting a detailed investigation into reported conduct). More specifically, the law firm Fieldfisher LLP assists us in handling alerts received.

- (e) to any other person, where you have given your prior consent to such disclosure.

4. How Do We Protect Your Privacy and Personal Data?

4.1 In accordance with this Statement, we will process Personal Data as follows:

- (a) Fairness: We are transparent about how we process Personal Data, and we will process it in compliance with applicable law.

- (b) Purpose limitation: We will process Personal Data only for specified and lawful purposes, and we will not process it in a way that is incompatible with those purposes.

- (c) Proportionality / Data minimization: We will process Personal Data in a manner that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. In addition, we encourage whistleblowers to provide only objective, factual, and directly relevant Personal Data related to the subject matter of the report.

- (d) Data accuracy: We take appropriate measures to ensure that the Personal Data we hold is accurate, complete, and, where necessary, kept up to date.

- (e) Data security: We implement appropriate technical and organizational measures to protect the Personal Data we collect and process about you. These measures are designed to provide a level of security appropriate to the risks associated with the processing of your Personal Data.

- (f) International data transfers: The Personal Data collected through our internal reporting channel is stored within the European Economic Area (EEA), and our service provider is also located within the EEA.

- (g) Data retention: We retain the Personal Data we process for as long as we have a legitimate need in relation to the purpose, in order to handle alerts and to protect the whistleblower as well as any persons or third parties involved. Beyond this period, we will delete or anonymize the data, or, if deletion is not possible (for example, where your Personal Data has been stored in backup archives), we will store it securely and isolate it from any further processing until deletion becomes possible.

Accordingly, the name, role, contact details of the whistleblower (including the company registration number), and of any person benefiting from protection and support measures will be retained until the statute of limitations applicable to the reported facts has expired.

Other Personal Data relating to alerts that have been verified but have not led to further action will not be retained for more than two months after the end of the verification process, unless disciplinary proceedings, judicial proceedings, or administrative proceedings have been initiated or are envisaged against the person involved or against the author of a malicious report. In such cases, the data will be retained until the end of the proceedings or until the limitation period for appeals has expired.

Personal Data that is clearly not relevant to the handling of a specific alert will not be collected or, if inadvertently collected, will be immediately deleted.

5. Your Data Protection Rights

5.1 You have the following data protection rights, which you can exercise by contacting us at dpo@ikanbi.com :

- (a) You may exercise your right to information and your right of access to obtain confirmation as to whether or not we process your Personal Data, to obtain information about the way your data is processed, and/or to obtain a copy of your Personal Data (provided this does not adversely affect the rights and freedoms of others, for example the confidentiality of data relating to the whistleblower). This means that it is not possible to make an access request for data relating to other individuals.

- (b) You may have your Personal Data rectified if it is inaccurate or incomplete.

- (c) In certain circumstances, you may request the erasure of your Personal Data (for example, if the processing is unlawful or if the data is no longer necessary for the relevant purpose). However, we may retain your Personal Data where it is necessary for the establishment, exercise, or defense of legal claims.

- (d)In certain circumstances, and in accordance with applicable data protection legislation, you may object to the processing of your Personal Data, or request that we restrict the processing of your Personal Data.
- (e) If you have a complaint or concern about the way we handle your Personal Data, we will endeavor to address your concerns. If you believe that we have not adequately resolved your complaint or concern, you have the right to lodge a complaint with a data protection authority regarding our use of your Personal Data. For more information, please contact your local data protection authority. Contact details for EEA data protection authorities are available here.

5.2 We will respond to the above requests without prejudice to our right and obligation to process alerts and to take appropriate action in response to them.

6. Updates to this Statement

6.1 We may update this Statement from time to time in response to changing legal, technical, or business developments. When we update our Statement, we will take appropriate measures to inform you, consistent with the significance of the changes we make. We will obtain your consent to any material changes where required by applicable data protection laws.

6.2 You can see when this Statement was last updated by referring to the "Last Updated" date displayed at the top of this Statement.

iKanbi Group SA

September 2025

iKanbi