Infobric Whistleblowing Policy

2025:1

Infobric Whistleblowing Policy

Infobric has implemented this Policy in order to ensure that Employees and external third parties can express their concerns in an effective and responsible manner. This Policy sets forth the routines on how to make a Report, procedures for Infobric's handling of whistleblowing Reports and the processing of Personal Data.

The Policy applies to Infobric and all Employees[1] as well as external third parties such as business partners, customers, suppliers, consultants, former or potential employees, or anyone else who is concerned with Infobric's business to report their concerns

1. PROCEDURES FOR REPORTING

Infobric is committed to maintaining a transparent business environment based on integrity and sound business practice. Infobric's expected conduct is set out in Infobric's Code of Conduct and associated policies.

To encourage and ensure that an Employee or any external third party who becomes aware of misconduct within the organisation raises his/her voice and reports the issue, Infobric has set up two ways of reporting.

Alternative 1: We expect that all our managers are open to receiving and handling concerns professionally. Therefore, as a main rule, you should always contact your immediate supervisor to report a suspected misconduct. If you do not feel comfortable talking to your immediate supervisor, you may contact that person's supervisor, anyone on the board, Legal or another person within the organisation you feel comfortable talking to.

Matters relating to poor management, inefficient systems or other operational aspects, alcohol or drug problems, petty theft at work, less serious work environment problems etc., should always be reported in accordance with Alternative 1.

Alternative 2: If you suspect that a misconduct has been committed you may use Infobric's whistleblowing system.

You can choose to Report anonymously through the whistleblowing system. However, it normally facilitates any subsequent investigation and handling of the matter if you identify yourself. Therefore, we encourage Employees to provide name and contact details when submitting a Report.

If you are an external third party and not a Infobric Employee and you would like to express your concern, please use the whistleblowing system.

[1] See Appendix A for a list of defined terms used throughout this Policy.

2. WHAT CAN BE REPORTED THROUGH THE WHISTLEBLOWING SYSTEM?

Infobric wants to identify, stop, and prevent violations of the law, our internal policies and regulations and other unethical behavior, including the following:

- Violations of local or international law, especially corruption, bribery, fraud, violations of anti-trust or competition law, export control and trade sanctions, money laundering and terrorist financing, financial statement fraud, smuggling of drugs, black market dealings and production/sales of counterfeit products, insider dealing, or unpermitted use of intellectual property by Infobric or a related third party;

- Human rights violations such as signs of modern slavery, child labor, human trafficking, forced, bonded or compulsory labor related to Infobric operations or a Infobric business partner;

- Non-compliance with safety and environmental compliance requirements, such as hazards regarding health, safety (including product safety) and security at the workplace, hazardous waste spills, discharges, or other environmental concerns;

- Non-compliance with Infobric internal policies or procedures such as Infobric Code of Conduct, or misuse of company assets, such as non-disclosed conflicts of interest, theft or misuse of company inventory, cash, equipment, supplies, or other assets, unauthorized disclosure of confidential information;

- Non-compliance with fair workplace principles or labor law including discrimination based on gender, gender identity, or expression, age, nationality, race, ethnicity, skin color, or cultural background, religion or beliefs, disability, genetics, or health information, including pregnancy, sexual orientation, or union affiliation, or harassment and threats, such as power and sexual harassment.

For the Policy to be applicable, it is required that there is a public interest in finding out about the misconduct. In most cases, the Policy does not apply to reporting of matters that only concern an employee's own working or employment conditions.

3. HOW TO REPORT A CONCERN THROUGH THE WHISTLEBLOWING SYSTEM

All Reports made through the whistleblowing system will be handled by Infobric's whistleblowing committee. The committee is comprised of Legal. If you do not want a certain person of the committee to be part of the handling of the Report, you may state that in your Report.

If you wish to make a Report through the whistleblowing system that fits the described prerequisites above, please use any of these links:

report.whistleb.com/sv/infobricgroup (Swedish)
https://report.whistleb.com/en/infobricgroup (English)
https://report.whistleb.com/no/infobricgroup (Norwegian)

You can also contact our whistleblower function via our switchboard, phone number +46 (0)36-340302.

Please report with honesty and in good faith. This means your Report should be based on facts and observations that you believe are true, and where you are not certain about your facts or observations, we request that you highlight your doubts and concerns in your Report. You do not have to have proof of your concern, but all Reports should be made in good faith.

Personal Data should only be included in the Report to the extent necessary. Sensitive Personal Data should not be included unless absolutely necessary.

4. THE HANDLING OF REPORTS

When the whistleblowing committee receives a Report, it will first assess whether the Report falls within the scope of the whistleblowing system or not. If not, the Report will be referred to the right function internally and the whistleblower will be notified. Further, if a member of the whistleblowing committee has an interest in the matter reported, that member will recuse him/herself.

When a reporter reports a concern through one of the designated reporting channels, we will provide the reporter with confirmation of receipt not later than seven days after the Report has been received. The form of such confirmation can be either oral or in writing.

The whistleblowing committee will review your Report and decide on appropriate measures. Further investigation into the matter may require the involvement of other group functions or external expertise, i.e. legal counsel, accounting firms, forensic firms, etc. It is only the committee that will have access to the Report.

The reported concern will be investigated as soon as practically possible.

Under our ordinary procedures, we will provide the reporter with an update regarding the status of the Report within 3 months after the confirmation of receipt.

When the investigation is closed, we will inform the reporter about the outcome of the investigation. Such information will typically be limited to high-level information, taking care to protect the privacy rights of affected individuals pursuant to our confidentiality obligations.

The above does not apply when it is unknown whom to provide the feedback to.

If you become subject of a Report the committee will inform you about it as soon as providing such information would not jeopardize the investigation.

All Reports will be handled with confidentiality. This means that the identity of the whistleblower and the handling of the Report will be kept confidential and disclosed strictly on a need-to-know basis. If deemed necessary, it might be communicated within Infobric, to the media, or others that a misconduct has been reported and is being investigated. Public authorities such as the police may also be informed in cases involving criminal offences.

The third party provider of the whistleblowing system, WhistleB, safeguards the anonymity of the whistleblower and ensures that all data is encrypted during transmission and in storage. WhistleB is certified under ISO 27001 to ensure the highest possible data security and privacy.

In follow-up activities, we consider the legal rights of the reporter as well as the person(s) concerned, any witnesses or other individuals named in the Report.

We are committed to managing all follow-up activities in a fair, impartial, and objective manner with respect for all person(s) involved, including the reporter, person(s) concerned and any other, e.g., witnesses. This also means that in the follow-up activities we will not involve persons who may have a personal conflict of interest in the reported matter.

5. PROTECTION AGAINST RETALIATION

No person will be subject to reprisal for reporting information about potential misconduct or compliance issues. Any retaliation for reporting suspected misconduct or participating in an investigation should be immediately reported to Infobric's General Counsel.

6. PROCESSING OF PERSONAL DATA

Reports made through the whistleblowing system are likely to contain Personal Data. The Personal Data may pertain to the person who has made the notification, and/or to a person suspected of the alleged wrongdoing and possible witnesses.

The following companies within the Infobric are jointly responsible (as joint data controller) for the processing of Personal Data with regards to whistleblowing cases.

Infobric AB	Framgången 1, SE-553 18 Jönköping, Sweden, info@infobric.se
TelliQ AB	Glasbruksgatan 1, SE-732 31 Arboga, Sweden, info@infobricfleet.se
AddMobile AB	Dockplatsen 1, 211 19 Malmö, Sweden, info@infobricworkorder.se
Hyrma AB	Glasbruksgatan 1, SE-732 31 Arboga, Sweden, support@hyrma.se
Jobsafe Edtech AB	Framgången 1, SE-553 18 Jönköping, Sweden, support@jobsafe.se
Infobric AS	Universitetsgata 10, 0164 Oslo, Norway, info@infobric.no
Infobric Time AS	Universitetsgata 10, 0164 Oslo, Norway, info@infobrictime.no
HMSREG AS	Universitetsgata 10, 0164 Oslo, Norway, support@hmsreg.com
BlastManager AS	Universitetsgata 10, 0164 Oslo, Norway, support@infobricblastmanager.no
Intershare AS	Kjøita 25, 4630 Kristiansand, Norge, info@infobric.no

i. What types of Personal Data can be processed?

The types of Personal Data which may be processed in conjunction with an investigation are typically the following:

- The name, position, and contact details (for example e-mail and telephone number) of the perspn who submitted the complaint and the individual to whom the complaint relates, as well as any witnesses or other individuals affected.
- Details of the misconduct of which the person reported is suspected.

Infobric will only process Personal Data which is correct and relevant to the investigation. Superfluous Personal Data will not be processed. Sensitive Personal Data may not be submitted unless essential for the reported issue and will be erased unless legal to process and deemed absolutely necessary for the investigation.

ii. Why is Personal Data processed?

Any Personal Data collected via the whistleblowing system will be processed for the purpose of administering and investigating allegations raised, and dealing with discovered misconduct, as described in this Policy and for statistical purposes.

iii. What is the legal basis for processing Personal Data?

The processing of your Personal Data is based on the legitimate interests pursued by Infobric. This means that Infobric is of the view that its interest in processing your Personal Data for the purposes listed above outweighs the privacy interest in the processing. In making this determination, we note that the processing of Personal Data is: (i) necessary to enable Employees and external third parties to raise serious concerns internally that may not be raised in the absence of a whistleblowing system; (ii) narrowly tailored to achieve the Infobric's legitimate interests; and (iii) in compliance with guidelines on whistleblowing issued by the relevant data protection authority (if applicable).

iv. Who has access to Personal Data?

Infobric takes both technical and organizational security measures to protect the Personal Data processed. The Personal Data collected will be processed only by those individuals at Infobric who are involved in the investigation. In this context, Personal Data may be transferred to a function within Infobric (such as internal audit), management, the board of directors, or other persons closely related to Infobric. In addition, investigation into the matter may require the involvement of external expertise, such as legal counsel, accounting firms, forensic firms, etc. Personal Data may also be disclosed to the police or other law enforcement authorities, or independent auditors for the same purpose. To the extent deemed necessary, it may also – for the same purpose – be transferred to affiliates or joint venture partners of Infobric. Any sharing of Personal Data is based on the same legal basis as for the processing of Personal Data of administrating and investigation allegations as such (please see section v above).

Your Personal Data may be transferred to countries outside the EU/EEA, which may offer a lower level of protection than within the EU/EEA. If so, Infobric will ensure that there are adequate safeguards in place – in light of the laws of the receiving country – to protect your Personal Data, such as signing a data transfer agreement including the Standard Contractual Clauses for data transfers between EU and non-EU countries, adopted by the EU Commission and which are available on the EU Commission's website.[2] For further information to which

[2] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

countries are transferred and the safeguards that Infobric has adopted to protect Personal Data, please contact us at the contact details above.

v. For how long is the Personal Data kept?

Personal Data which is collected and processed will not be retained longer than necessary. Complaints, reports, and information regarding misconduct which have been investigated will be deleted within two months of the conclusion of the investigation or, if the investigation results in action being taken against the individual who has been reported, when the information is no longer needed for the purpose of carrying out an investigation and taking action. If it is decided that no investigation will be initiated, the information will be deleted immediately after such decision has been made.

vi. What are your rights?

If we receive a Report which includes your Personal Data or if your Personal Data is collected within an investigation, we will provide you with information if possible. However, if the provision of such information may compromise the investigation, you will instead receive information as soon as possible after the investigation has reached a stage where such risk no longer exists.

You are entitled to know what Personal Data we are processing about you, and you can request a copy of such data. However, note that to the extent disclosure of your Personal Data may compromise an investigation, we may not be able to meet your request. You are entitled to have incorrect Personal Data about you corrected, and in some cases, you may request that we delete your Personal Data. You are also entitled to object to certain processing of your Personal Data, and request that the processing of your Personal Data should be restricted.

If you have any questions regarding the processing of your Personal Data or wish to exercise any of the rights stated above, please write to the data controller at the contact details provided above.

You have the right to lodge a complaint regarding how we process your Personal Data to the relevant data protection authority or similar body within your jurisdiction.

7. RESOURCES

This Policy does not address every possible issue that may arise concerning the use of the whistleblowing system. If any questions or concerns arise regarding this Policy or its application to a specific situation, Employees are expected to seek guidance from their Manager and, if necessary, Infobric’s General Counsel.

Appendix A – Definitions

Employee	Any director, officer, contractor, or temporary or permanent employee of Infobric as well as job seekers.
Policy	This Whistleblowing Policy.
Personal Data	Any information relating to an identified or identifiable natural person.
Report	the oral or written communication about actual or suspected infringements of Infobric Code of Conduct, applicable local or international laws and regulations.
Sensitive Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.