

Iptor Whistleblower Policy

1. PURPOSE OF THE WHISTLEBLOWER SCHEME

Iptor, as part of the GSG Genii Software Group, wants an open corporate culture where everyone can come forward freely and report suspected irregularities or illegalities concerning Iptor's employees, management, board of directors and other stakeholders.

Iptor's employees will often be the first to detect irregularities or fraudulent behavior. However, it often turns out that most people are reluctant to go ahead with their suspicions. Recognizing this, Iptor has chosen to set up a whistleblower scheme via the GSG HR portal "Bob" – called **Your Voice** - where all employees can report violations or omissions – anonymously if so chosen - in relation to legislation as well as other serious and sensitive matters.

The whistleblower scheme aims to increase the ability of Iptor employees to:

- express an opinion on illegal or objectionable facts.
- protect those who report information to the whistleblower portal.
- detect maladministration.

The whistleblower scheme is supplementary to the direct and daily communication at Iptor about errors and unsatisfactory conditions, so problems should therefore be addressed in the first instance by contacting, for example, the employee's immediate manager, a union representative or directly management.

2. SCOPE OF THE WHISTLEBLOWER SCHEME

The Iptor whistleblower scheme is set up in accordance with the EU directive and allows employees to make anonymous reports if there is a reasonable suspicion of serious and objectionable facts or illegalities that could cause punitive, financial loss or serious damage to Iptor's reputation.

3. WHO CAN REPORT

All employees, board members or business partners can report anonymously or choose to inform Iptor of their identity and contact information. Both current and former employees can make a report.

Likewise, the whistleblower portal allows external stakeholders such as customers, suppliers, and business partners to report via an external link to Your Voice from Iptor's homepage.

4. WHO CAN BE REPORTED ON

The report may relate to the following categories of persons:

- Employees in Iptor, i.e., where an employment relationship has been established between Iptor as an employer and the employee as an employee. The form of employment is not relevant (permanent, part-time, hourly, temporary, former)
- Directors
- Business partners and suppliers
- Basic system errors that cannot be attributed to a specific person or person.

Only persons associated with Iptor may be reported via the Iptor Whistleblower portal.

5. WHAT CAN BE REPORTED

The report shall relate to serious offences, offences or other serious circumstances or suspicions thereof. Only:

- Serious and/or criminal offences such as theft, embezzlement, fraud, bribery, corruption, accounting fraud/manipulation, improper use of assets, misuse of financial resources, etc.
- Serious issues relating to discrimination, violence, assault, and harassment.
- Serious and repeated violation of internal guidelines and procedures.

Knowledge or reasonable suspicion of such facts is assumed.

Inquiries related to the employment relationship, e.g., absence, difficulties with cooperation, smoking, alcohol, clothing, salary conditions, etc., as well as matters that are **not** serious, should **not** be reported through the whistleblower portal, but handled via, for example, the nearest manager, human resources department, union representative, etc.

To the extent possible, the alert shall be documented by attaching relevant documents in digital form.

6. REPORTING PROCEDURE

Reports can be made anonymously by using Your Voice in the GSG HR Bob portal which can be accessed in the portal or via the external link found on Iptor's homepage.

No other channel should be used, as a report typically contains confidential information that may not be sent over the open Internet without encryption.

7. CONFIDENTIALITY AND ANONYMITY

All information is treated confidentially and with discretion.

If a report is made anonymously, it is essential that no contact information (name, email address, telephone number, etc.) is provided by the reporter and that the reporter is aware of removing metadata from files by attaching documentation, and that the reporter does not provide information that can be traced directly back to him or her.

Should an investigation be subject to an external body, e.g., the police, Iptor may be forced to disclose the identity of the reporter, if Iptor is aware of it. The reporter will always be informed before any external body is involved.

If information is reported from Iptor's network or other monitored network, there may be a risk that visits to the whistleblower portal will be logged internally as part of the regular logging of user activities. This risk can be avoided by entering the web address itself in a browser on a private or public computer that is not connected to a monitored network.

Your Voice is designed to remove or restrict the storage of information when visiting and using the GSG Bob portal.

8. PROCESSING OF REPORTS

The submitted reports via Your Voice are directed to the company and accessed by a few trusted managers or HR employees. The reporter chooses between representatives in the chosen category when delivering the report. The report goes to one individual, but notification is sent to all in the group.

An initial review of the report in the Iptor representative group is carried out to assess whether it falls within the scope of the whistleblower scheme, whether there is a need for a proper case management of the relationship, or whether the report can be deemed as manifestly baseless (e.g., if the report deals with matters or is reported by a person not covered by the whistleblower scheme).

If there are grounds for admissibility of the alert, a closer examination of the facts shall be initiated. If needed, assistance with the treatment is obtained, e.g., from legal or other external advisors.

9. PROCESSING OF PERSONAL DATA

The processing of personal data provided, including collection, storage and, where appropriate, disclosure, is subject to applicable data protection law rules.

The processing of the data is subject to Iptor's legitimate and objective interest in processing personal data submitted in the alert – and the processing is considered to exceed the interest of the data subject. The processing is thus carried out in the light of the balancing rule laid down in Article 6(1)(f) of the Data Protection Regulation.

10. HANDLING OF REPORTED CASES

It is possible to report anonymously and subsequently communicate anonymously with Iptor. After initial reporting via Bob Your Voice, all communication takes place in the portal via email between the Iptor representative and the (anonymous) whistleblower. The fictive email constructed by Bob for this purpose is to ensure that the real email used by the reporter is not shown to the Iptor representative but allows any additional questions to be put to the reporter without knowing his or her identity. This is a way of ensuring that the alert is adequately reported for it to be processed.

The email setup will also be used to communicate any conclusion of the case to the reporter. The following deadlines apply:

- Before seven days, receipt of the report shall be communicated.
- The procedure is carried out as soon as possible and it is sought that the procedure does not exceed three months.
- The conclusion of the case is communicated to the reporter via anonymous email.
- As a rule, all closed cases are deleted within 6 months of the reporting date. This is a manual process for the individual HR representative in Bob.

11. THE PERSON REPORTED ON

Unless specific and justified investigative considerations apply, the person concerned shall be notified of the handling of the case once the report has been received and an investigation has been launched.

12. RIGHTS

Reports submitted in good faith will not have adverse consequences for the reporter. Reports filed in bad faith or filed to harass or harm the person covered by the reported information, may have consequences for the reporter (e.g., lead to police reporting or have employment law consequences).

Persons submitting information to the whistleblower scheme will, as a rule, be informed of the handling of the case and, where appropriate, of the outcome.

13. DELETING DATA

If the report does not fall within the scope of the whistleblower scheme, or if the report is baseless, the data will be deleted immediately.

Personal data is also deleted when it is no longer necessary to keep, including when the investigations have been completed.

The general deletion rules also apply. If, based on the information collected, disciplinary action is taken against a staff member, or if there are otherwise reasons why it is objective and necessary to keep information about a staff member, the information will be kept in his HR records.

14. QUESTIONS

All questions relating to the whistleblower scheme can be directed in writing to Iptor HR using privacy.notification@iptor.com.

Iptor HR
March 2024