WHISTLEBLOWING POLICY

Dated 5 October 2022

PROBI AB

This Policy has been adopted on 5 October 2022 by CFO and VP HR & Sustainability

1. INTRODUCTION

Probi AB, including all companies in the Probi AB group of companies ("**Probi**" or "**we**"), shall conduct its business in a responsible and sustainable manner. We expect our employees, including directors of the board ("**you**"), to act in accordance with applicable law, principles on business ethics, and internal policies and procedures with high integrity.

If you suspect that Probi, or any of its subsidiaries, or anyone acting on our behalf, is acting in violation of applicable law or our internal policies and procedures, you are required to report such (suspected) misconduct.

If the suspected misconduct is of serious nature and may be reported in our whistle-blower channel (see Section 3), then the whistle-blower channel must be used. This is important to you, because by reporting in the whistle-blower channel, you will by operation of law gain special protection. This is also important to us, since we expect reporting into the whistle-blower channel to provide the best conditions to investigate your report and to follow-up with you.

If the matter cannot be reported in the whistle-blower channel, you should turn to our group CFO or group VP HR & Sustainability, or any other manager or member of the board that you trust.

If you do not feel comfortable turning to any of the above-mentioned alternatives, you have instead the opportunity to report suspected misconduct in the external reporting channels of relevant authorities. See more about this in Sections 4 and 7.

2. WHO CAN SUBMIT A REPORT?

Our whistle-blower channel is available to all employees and directors of the Probi group of companies. Also other individuals who work with us under our control, such as directors, trainees, volunteers, hourly employees (*Sw. timanställda*) and self-employed persons, can submit a report in the whistle-blower channel.

We also make the whistle-blower channel available to customers, suppliers and other business partners.

A person, who in good faith and on reasonable grounds suspects a certain misconduct and submits a report via our whistle-blower channel, shall not be subject to any retaliation, regardless of the outcome of the subsequent investigation. However, deliberate reporting of false or malicious information is a serious disciplinary offence and not tolerated.

3. WHAT CAN A REPORT BE ABOUT?

By law[1], reports in the whistle-blower channel may concern reporting within a work-related context of (i) serious (suspected) misconduct in the *public interest* to uncover; or (ii) (suspected) acts or failure to act in breach of or contrary to Union law, i.e. EU law and implementing acts.

[1] The Swedish Whistleblower Act (*Sw. lag om skydd för personer som rapporterar om missförhållanden*)

This may include (*examples*):

(a) Illegal activities of a serious nature

(b) Financial fraud, such as incorrect accounting, violations of internal control procedures, misappropriation of assets or fraud

(c) Bribery and corruption, for example, promising, taking or giving of bribes

(d) Violations of anti-trust laws (e.g. exchange of price sensitive information or illegal cooperation between competitors)

(e) Material violations of Probi policies or conflicts of interest

(f) Serious threats to the environment, health and safety, including work environment

(g) Material breaches of privacy regulations, personal data breaches and network and information security

(h) Activities that are otherwise seen as seriously inappropriate behaviour, for example, discriminatory work routines, harassment and other serious unethical conduct, the use of child labour and human rights violations

(i) Other serious misconduct which concerns Probi's vital interests, individuals' life and health, or misconduct for which there is a public interest in its uncovering

Matters such as poor leadership, alcohol or drug problems, petty theft at work, less serious work environment problems or offenses committed by persons that do not hold senior or key positions and similar, can normally not be reported (and handled) in the whistle-blower channel.

The information in a report should always be submitted in good faith and, to the extent possible, fact based. Personal data (*i.e.* any information relating to an identified or identifiable individual) should (only) be included in the report to the extent it is necessary.

4. HOW DO YOU SUBMIT A REPORT?

A report is submitted in the whistle-blower channel by using the confidential whistle-blower channel available on Probi's website: https://probi.integrity.complylog.com/

You may also contact designated persons directly.

Or you may report to an external channel maintained by a competent authority, see more about this in Section 7.

You have a right to request a physical meeting. Such meeting may be requested in the whistle-blower channel, in which case such a meeting shall take place without undue delay.

You may submit a report in the whistle-blower channel anonymously. However, you are encouraged to provide contact details, which provides the best conditions to investigate your report and to provide feedback to you.

If you wish to report (suspected) misconduct that is not reportable in the whistle-blower channel, you are asked to contact our group CFO or group VP HR & Sustainability, or any other manager or member of the board that you trust. If either of these persons receive a report that they deem to fall within the scope of the whistle-blower channel, it is their duty to inform you that the report should be submitted to the whistle-blower channel, or the manager must report the (suspected) misconduct into the whistle-blower channel himself/herself.

5. WHAT HAPPENS WHEN YOU HAVE SUBMITTED A REPORT?

Once you have submitted a report, it will be received by specially designated and competent persons (*Sw. behöriga personer*) appointed by Probi AB[2] to manage the whistle-blower channel, including the receipt of reports, the investigation of reports and to have contact with and provide feedback to the reporting person.

The designated persons appointed by Probi AB are: Basudha Bhattarai Johansson (VP HR & Sustainability) and Henrik Lundkvist (CFO)

Within **seven days** of receiving your report, you will receive a confirmation that your report has been received, unless you have declined such confirmation or there is reason to believe that a confirmation could reveal your identity.

The designated persons will initially assess if your report covers such irregularities that can be processed in the whistle-blower channel. If the assessment is made that the report cannot be processed in the whistle-blower channel, you will be informed hereof within seven days of receiving your report, including further information about who you can turn to instead.

If your report includes such irregularities that can be processed in the whistle-blower channel, the designated persons will then review your report and decide on appropriate measures to investigate the suspected irregularities. If you have provided contact information, you may be contacted to answer follow-up questions.

Investigations may require the involvement of other internal functions or external expertise, such as IT expertise, legal advisers, auditors or forensic investigating expertise.

If the investigation concludes any misconduct, Probi may take disciplinary actions against individuals involved in misconduct. Such disciplinary actions may constitute reprimands up to and including termination of employment. Probi may also report any misconduct to the police or other relevant authorities and may take legal action against individuals involved in such misconduct. Furthermore, Probi may implement remediating actions, such as training, new or updated policies, etc. if found necessary.

No later than three months after having received confirmation of receipt of your report, the designated persons will provide you with appropriate feedback on investigative measures taken. You will also receive a notification when the investigation is complete. The communication will not necessarily contain the results of the investigation.

---

[2] Pursuant to chapter 5 paragraph 5 of the Swedish Whistle-blower Act (Sw. *lag om skydd för personer som rapporterar om missförhållanden*)

If a designated person is affected by a report or otherwise has a conflict of interest, that person will not participate in the investigation or otherwise be allowed to take part in the matter.

6. WHAT ARE YOUR RIGHTS AS A REPORTING PERSON?

Anonymity and confidentiality

Probi's whistleblowing application, IntegrityLog, is provided by the company ComplyLog. IntegrityLog provides an application for reporting and receiving reports that ensures the confidentiality of the reporting person and other parties mentioned in the report and can only be accessed by the designated persons.

You may submit your report anonymously. If you choose to report anonymously, the designated persons will not try to find out who submitted a report. Although it is possible to remain anonymous, we encourage you to provide contact details as anonymous reports are often more difficult to investigate.

Even if you do not choose to remain anonymous when registering, your identity will be treated with strict confidentiality and reports kept strictly confidential. The persons who handle your report may not disclose information that may reveal your identity or the identity of any other person who appears in the case, other than for authorized purposes.

If information that can identify you is proposed to be lawfully disclosed, you will be informed of this, unless such information obstructs or impedes the purpose of the investigation or measures.

Protection against retaliation

It is strictly forbidden for Probi or anyone with our organization, to prevent or attempt to prevent you from reporting suspected misconduct.

Probi also does not allow any form of retaliation against anyone who in good faith reports a suspected misconduct in accordance with this Policy. No employee shall be retaliated against or subjected to disciplinary action, due to the fact that he or she has acted in accordance with this Policy. The prohibition to retaliate extends also to anyone who assists you in reporting (for example, a union representative) or against a legal entity that you own, work for or is otherwise connected to.

If you believe that you have been the subject of such treatment as described above, you must report this in the whistle-blower channel as soon as possible.

Retaliation against a person who in good faith has reported a concern in accordance with the Policy, is a serious disciplinary offence and not tolerated.

No liability

A reporting person who in good faith reports a misconduct in accordance with this Policy and who has reasonable grounds to believe that a report is necessary to disclose the misconduct shall not be held liable for having breached the duty of confidentiality or having acted in breach of laws in the collection of information. Certain exemptions are specified in the Whistle-blower Act.

The content of this Policy does not restrict any rights under the constitutional freedoms of providing and retaining information (Sw. *meddelar- och anskaffarfrihet)*.

7. HOW TO SUBMIT A REPORT IN EXTERNAL WHISTLEBLOWING CHANNELS

You also have a right to report suspected misconduct to any of the external whistle-blower channels established by certain authorities or EU institutions, bodies, offices or agencies. These authorities are tasked with receiving, following up and providing feedback on reports of malpractice within a designated area of responsibility.

If you wish to submit a report to an external whistle-blower function, you should first contact the authority responsible for the relevant area.

8. HOW IS PERSONAL DATA PROCESSED?

Categories of personal data and data subjects

Reports, although submitted anonymously, may contain personal data relating to the sender and individuals included in the report. Any investigation may also collect personal data on the persons concerned and any third persons involved. Such personal data may consist of name, address, gender, nationality, role or function, contact information, details of the reported event, measures taken investigation reports and other types of data collected, including via telephone logs, data files, audio files, IP addresses and other technical data as well as e-mail. alleged misconduct, and types of other personal data included in the report, and information collected within the investigation, e.g. phone records, computer files, correspondence, etc.

Depending on the nature of the report, sensitive personal data may be processed, such as information about ethnic origin, political opinions, religious or philosophical beliefs, union membership and information about health or sex life. When submitting a report, the whistleblower should as far as possible avoid disclosing such sensitive personal data that is not relevant to the report. A report may also lead to processing personal data about actual or suspected criminal convictions and offences.

Purposes of the processing and legal basis

Personal data is processed primarily for the purpose of handling and investigating a follow-up case. Personal data processed for this purpose may also be processed for the purpose of fulfilling a disclosure that: (i) is necessary to take action in connection with what has emerged in a report; (ii) is necessary for reports to be used as evidence in legal proceedings; and (iv) is in accordance with applicable law and regulation. This processing, as well as processing of actual or suspected criminal convictions and offences, is based on our statutory obligations to provide a whistleblowing service.

The legal basis for our processing of sensitive personal data is that the processing is necessary in the interests of a substantial public interest, on the basis of Union law or the national law of the Member States. In some cases, we may also process sensitive personal data when necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law, in so far as it is authorised by Union or Member State law.

In some cases, we may also process personal data in order to take further measures in connection with a report. We then rely on our legitimate interest in processing personal data in order to be able to take such action. To the extent we need to process sensitive personal data or data concerning actual or suspected criminal convictions and offences for this purpose, this is done on the basis that it is necessary to establish, assert or defend a legal claim.

Deletion of data

Personal data will only be stored for as long as is necessary to investigate a report and to take relevant follow-up measures in relation to the results of such an investigation.

Personal data that is processed in relation to an investigation is in any case never processed longer than two years after the investigation was closed.

Excess personal data and personal data that are not relevant to the reported event will be deleted or anonymised as soon as possible.

Personal Data Controller

Probi AB, reg. no. 556417-7540 and address Ideongatan 1A, 223 70 Lund, is the data controller of personal data processed in the whistle-blower channel.

Sharing with third parties

Access to personal data is reserved for the designated persons who handles the information confidentially. However, in order to fulfill the purposes of the processing of personal data (i.e. to investigate the reported misconduct), the personal data may be shared with third parties, such as external legal advisers, audit firms, forensic investigators or other service providers that are necessary to detect, investigate and remedy serious breaches. The company may also share personal data with the police and / or other relevant authorities, supervisory bodies or courts to safeguard our interests or exercise our rights.

Personal Data Processor:

IntegrityLog, Holländargatan 17, 111 60 Stockholm, Sweden, is responsible for the whistle-blower application, including processing of encrypted data, such as whistleblowing messages. Neither IntegrityLog nor any sub-suppliers can decrypt and read messages. As such, neither IntegrityLog nor its sub-processors have access to readable content.

Information to data subjects and rights of data subjects

If we receive a report that contains personal data concerning you or if personal data is collected during an investigation, we will, if possible, inform you. If the provision of such information may jeopardize the investigation, you will instead be informed as soon as possible after the investigation has reached a stage where such risk no longer exists.

You may exercise your rights of access, of rectification, deletion and of opposition, as well as of limited processing of your personal data in accordance with the local data protection legislation. These rights are subject to any overriding safeguarding measures required to prevent the destruction of evidence or other obstructions to the processing and investigation of the case. For instance, please note that to the extent that the disclosure of personal data may jeopardize an investigation, we will not be able to fulfil the request.

Data is stored within the EU only.

If you have questions regarding how Probi processes personal data about you, you may contact us at the contact information stated above. If you have any objections or complaints about the way we process your personal data, you have the right to file a complaint with the Swedish Authority for Privacy Protection (Sw. *Integritetsskyddsmyndigheten*).