Tibber whistleblowing program policy

1 Introduction

Tibber needs to be trusted. Tibber wants to be trusted. If our customers, employees, partners, and other stakeholders don't trust anymore, Tibber is no more!

Tibber strives for transparency and a high level of business ethics. We believe that openness and transparency within Tibber are key to preventing, detecting, and responding to irregularities and promoting a healthy working environment. Therefore, we encourage anyone who has a concern to raise it with us.

The whistleblowing program and associated Whistleblowing Channels provides an opportunity to report suspicions of serious misconduct within Tibber; any incident that violates law, our internal company policies and/or our ethical standards.The Whistleblowing Channels provides an opportunity to report observations anonymously.

A report of an observation through the Whistleblowing Channels will be received and managed by **Tibbers' whistleblowing committee**, chaired by Tibber's Director of Legal.

2 Purpose

The purposes are to:

- provide the person who reports with support and guidance when the person wishes to report an observation of severe misconducts/censurable conditions that have occurred or are very likely to occur in our organization. It applies to all employees or other persons who are, or were, connected with our business, without a risk of being subject to retaliation;
- ensure that observations are handled with fairness, objectivity, and confidentiality;
- provide the possibility to whistleblow anonymously;
- at least comply with relevant whistleblowing legislation.

3 Who can report an observation

The whistleblowing program is established for Tibber employees (including temporary employees, interns, etc.), consultants, job applicants or Tibber officials (for example board members), and persons that have had these roles before.

4 What to report

The whistleblowing program can be used to report suspected misconduct when a misconduct becomes apparent in Tibber's organization. Suspected misconduct or censurable conditions means conditions that are considered acts or omissions that occurred (or are most likely to occur) in Tibber's organization which are considered harmful to the public interest. This could include conditions against, but not limited to, Tibber's Code of Conduct, applicable laws, and regulations in the countries where Tibber operates, or generally accepted ethical norms. Relevant laws and regulations include the EU

Directive on Whistleblowing and associated national legislation. In Germany, a whistleblower can also report on violations of German criminal law and administrative offense law.

Examples of what to report (but not limited to):

- Bribery, corruption, money laundering and terrorist financing
- Unlawful conduct or unfair competition
- Violation of environmental and occupational safety legislation
- Violation of privacy and personal data
- Violation of product safety legislation
- Interference with the right of workers to organize
- Unilateral weakening of work tasks
- Violation of other laws or our ethical principles
- Violation of the organization's Code of conduct
- Harassments, bullying and other unacceptable behavior; abuse of authority
- Danger to life or health
- The gray economy (neither taxed nor monitored by any form of government, "under the table")

4.1 Good faith

Reports must be made in good faith. Deliberate false reports are prohibited and may result in legal action.

Whistleblowers do not need proof of their suspicion, but do, however, need reasonable cause to assume that the information is true at the time of reporting.

Reporting motivated solely by a desire to harm Tibber or its reputation, without due cause, affects the working environment or Tibber's employees negatively, are not worthy of notifications.

5 How to report

We provide three Whistleblowing channels:

- Tibber's digital reporting tool (or use https://app.falcony.io/tibber-wb/links/whistleblowing-external in your browser). By reporting an observation through the digital tool, you have the option to remain anonymous. Available 24/7.
- Letter to: **Director of Legal**, Tibber AS, Hafstadvegen 38, 6800 Førde, Norway.
- Employees can report via internal channels.

Concerns can also be reported to competent EU and/or national authorities or organizations.

6 Anonymity

The Whistleblowing Channels allow the whistleblower to report and remain anonymous by using:

> **The digital web-based tool:**
> The whistleblower can submit an observation easily and securely by using our digital tool. This reporting tool is provided by an external service provider, Falcony, a supplier that guarantees quality and reliability. The system is web-based and encrypted. After submitting

an observation, the whistleblower will receive an anonymous username and password with which he or she can log in to the service and communicate with the whistleblowing committee, and continue to be anonymous. All members of the whistleblowing committee will receive the observation.

All communication between the whistleblower and Tibber is transmitted through an encrypted connection which prevents unauthorized persons access to the reported observation and its content. The solution does not store data with traceability back to the whistleblower (unless the whistleblower provides contact information in the reporting form). The technical solution does not log IP addresses, browser information, “cookies” or other hardware details of the sending device (PC, phone, tablet etc.).

The web solution is a cloud based SaaS (Software as a Service) and is administered through an interface with high data security requirements, including limited physical access to servers, 24 hours monitoring of security events and comprehensive application security.

The web solution utilizes the TLS (Transport Layer Security) protocol with 256-bit AES encryption, which ensures that unauthorized parties may not gain access to information which is exchanged between the whistleblower and Tibber’s web solution.

Letter:
The whistleblower can send a letter to the **Director of Legal**, Tibber AS, Postboks 20, 6801 Førde, Norway. The Director of Legal will be responsible for opening the letter and sharing it with all members of the whistleblowing committee. Note that this channel limits the whistleblowing committee to correspond with you with reference to the observation.

It is strictly prohibited for all Tibber employees and other Tibber representatives to attempt to determine the identity of a whistleblower. Any such confirmed attempts will lead to disciplinary sanctions.

If the whistleblower chooses to identify themselves to Tibber, the whistleblowing committee will still treat the identity as confidential and with utmost care and only reveal it to other persons if necessary and with the consent of the whistleblower.

7 Observation management

Each reported observation will be taken seriously. Proper and adequate investigation measures will be decided and conducted. When handling an observation Tibber will always follow the principles of fair and objective process, confidentiality, protection of personal data, protection of sources and, protection of the person who reported the observation against retaliation. Managers and/or employees, only those necessary to manage the reported observation, will be involved. If necessary, we will in addition use an independent third party to help out with the investigation and assessment.

Any person that is or could be part of the objective of an observation will not be participating in any investigation or observation management. If such a person is part of the whistleblowing committee, that person will be excluded from any further observation investigation and management. If you find it inappropriate that one or several members of the whistleblowing committee, for any reason, should be aware of the reported observation at all (prevent evidence to be destroyed, etc.), we ask you to either send a letter and include this information in the observation (so that the recipient of these letters can

take appropriate measures before sharing the information further) or reach out to a member of the committee.

A final report on an investigation shall include (i) a brief description of the investigation methodology/approach, (ii) a summary of the relevant facts identified (incl. reference to the supporting documentation, (iii) a concrete assessment of the case and whether the reported censurable conditions have been confirmed, and (iv) conclusions and recommended measures and/or reactions.

In certain circumstances, the whistleblowing committee may decide not to investigate the reported observation. This can be the procedure, for example, in the following situations: the information obtained is insufficient in order to carry out an adequate investigation and no further information is available, the observation is reported in the wrong channel (in which case the reporting person is directed to report the matter to the correct party), the observation is not provided in good faith, or if an investigation has already been made. If the observation is reported anonymously, the whistleblowing team is prevented from further investigation of the identity of the reporting person. In case of an anonymous observation, such an observation may risk being dismissed if, for example, the information obtained is deemed insufficient in order to initiate an investigation or if the veracity of the information provided cannot be reliably established.

The general rule is that a) upon receiving an observation, we will confirm that we have received it within seven (7) days and b) you should then have relevant feedback, within a reasonable timeframe not exceeding three (3) months, about the investigation and related actions.

8 Protection against retaliation

No one, anonymous or not, shall suffer from retaliation for reporting misconducts/censurable conditions described in this policy. Whistleblowers who report an observation in good faith will not face any form of retaliation, even if the observation turns out to be mistaken/not true. Colleagues or relatives of reporting persons and legal entities that the reporting persons own, work for or are otherwise connected within a work-related context, are also entitled to protection against retaliation. The whistleblowing committee may therefore follow up on this with the reporting person sometime after that the investigation has been closed.

The EU Whistleblowing Protection Directive highlights a number of actions that might be classed as retaliation including obvious financial penalties: change in duties, working location, or contractual status; change in salary; and disciplinary penalties. It also highlights discrimination and damage to reputation, with social media as a possible source of retaliatory behavior.

It is also prohibited to hinder or attempt to hinder a whistleblower from reporting information about a misconduct.

Any confirmed retaliation or hindering will lead to disciplinary sanctions.

9 Entry into force

This whistleblowing program enters into force with immediate effect together with the introduction of the whistleblowing committee and the Whistleblowing channels.

The policy is approved by the whistleblowing committee and they have the responsibility to review the program and suggest adequate changes on a regular basis. Owner of this policy is the Director of Legal and it constitutes a part of the Tibber compliance program.

The Leadership team in Tibber has been informed about the whistleblowing program policy.

Privacy notice for Tibber whistleblowing program

1. CONTROLLER

The Controller for this process is any of the Tibber group entity that a report concerns: **Tibber AS** (916 276 338), Postboks 20, 6801 Førde, Norway (*mother company in the Tibber Group*); **Tibber Norge AS** (917 245 975), Postboks 20, 6801 Førde, Norway; **Tibber AB** (559047-8532), Vattugatan 17, 111 52 Stockholm; **Tibber Deutschland GmbH** (HRB208753B), Strelitzer Str. 60, 10115 Berlin; **Tibber Netherlands B.V.** (80004245 (KvK)), Herengracht 420, 1017BZ Amsterdam; **Tibber Oy** (3133529-2), Lautatarhankatu 10, 00580 Helsinki.

2. PURPOSE AND LEGAL BASIS

Purpose

The whistleblowing program is designed to give all employees of the Group, as well as external stakeholders, a means to report suspected cases of wrongdoing. The digital tool used as one report channel in the program gives the reporter the possibility to remain anonymous.

Personal data needs to be processed in order to collect and investigate such observations, and to decide on and implement any resulting measures.

Abuse of the whistleblowing program is prohibited and may result in legal action.

The controller is committed to protecting the data subjects' privacy and to only using personal data collected by means of the whistleblowing program as permitted by data-protection laws and good data protection practice.

Legal basis

The processing of personal data pertaining to the subjects of whistleblowing observations and the persons responsible for processing the observations is based on the controller's legitimate interest (GDPR, Art 6.1(f)). We have assessed and deemed that our interests are not overridden by the interests, fundamental rights and freedoms of the data subjects involved. The processing is also necessary for compliance with a legal obligation (GDPR, Art 6.1(c)). All processing is based on Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the

protection of persons who report breaches of Union law (OJ L 305/34 of 26 November 2019). The processing of special categories of personal data is necessary for the purposes of carrying out the obligations of the controller in the field of employment law (GDPR, Article 9.2(b)).

3. DATA SOURCES

Potential reporters include employees of the Group as well as external stakeholders. The controller also collects information that is necessary for investigating reports of wrongdoing from the interested parties themselves as well as from other individuals or organizations that may be involved.

4. CATEGORIES OF DATA SUBJECTS AND DATA

4.1 Reporters

As a rule, reporters using the digital tool report their observations/concerns anonymously. Some reporters include personal information (such as their name, location and contact information). Some observations contain pictures or video footage. Information provided by reporters themselves may also contain special categories of personal data (such as information about a person's health). The circumstances of the case may make it possible to identify the reporter indirectly, even when the observation is reported anonymously. Reporters reporting in a meeting situation can not be anonymous.

4.2 Subjects of observations

Observations of wrongdoing may contain information about third persons (such as their name, location or pictures), their behavior and circumstances as well as other personal information. Some observations may also contain special categories of personal data (such as information about a person's health).

4.3 Compliance committee and investigating parties

The following personal data are collected from the persons responsible for processing whistleblowing observations: name, title, username, log data.

5. ACCESS TO AND DISCLOSURE OF PERSONAL DATA

Only employees specifically assigned by the controller to process whistleblowing observations and investigate reported observations have access to the personal data relating to such observations.

The administrator of the controller's digital reporting tool is an external service provider (Falcony). The controller and the service provider have signed an agreement to ensure that the service provider only uses personal data collected by means of the whistleblowing program as permitted by the applicable data protection laws.

Personal data will be disclosed to affiliates in the Tibber group (that will process it as Controller) and when relevant to third parties, such as external law firms or similar, and relevant authorities or external auditors, as per the law.

6. TRANSFER OF PERSONAL DATA TO NON-EU/EEA COUNTRIES

The external service provider of the digital reporting tool has subcontractors who provide technical data processing services and some of whom are based in the United States and thereby outside of the EU.

Tibber has implemented the appropriate contractual safeguards to ensure adequate protection of any data transferred to non-EU/EEA countries as well as compliance with the laws governing the processing of personal data and stipulated that the service provider incorporate the standard contractual clauses for data transfers adopted by the Commission as referred to in Article 46.2(c) GDPR into its own subcontracting agreements.

7. STORAGE

As a rule, data are kept for no longer than two (2) years after the end of each investigation. Longer storage periods may be necessary due to mandatory legal obligations arising from, for example, criminal procedure or occupational safety laws.

8. RIGHTS OF DATA SUBJECTS

When we are processing your personal data, you have some rights. You have, for example, the right to have access to your personal data or the right to have your personal data corrected. Here you can read more about your rights and how you do when you want to exercise any of your rights.

(a) Request access to your personal data. Upon your request, Tibber will confirm whether we are processing your personal data and provide you with information on how we process the personal data. If requested, we provide you with a copy of that personal data. You will not have to pay a fee to access your personal data (or to exercise any of the other rights).

(b) Request correction of the personal data that we hold about you. By having access to personal data, you may be able to ensure the accuracy of your personal data. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us. Some data may be needed to process for historic reasons, i.e. may not always be possible to correct fully.

(c) Request deletion of your personal data. This enables you to ask us to delete or remove personal data, which we have no purpose for continuing to process. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

(d) Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

(e) Request restriction of processing of your personal data unless we demonstrate compelling legitimate grounds for the processing. This enables you to ask us to suspend the processing of your personal data (i) if you want us to establish the data's accuracy, (ii) where our use of the data is unlawful, but you do not want us to erase it, (iii) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims, (iv) if you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

(f) Request to object to have automated decision-making and profiling as you have the right to not be subject to decisions based solely on automated processing of your personal data, including profiling, that affect you, unless such processing is necessary for entering into, or the performance of, a contract between you and us or you provide your explicit consent to such processing.

(g) Request the transfer of your personal data to you or a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format, provided that the information requested to be transferred is provided by you, is processed on the basis of fulfilling an agreement or based on consent, and provided that the processing of personal data is carried out by automated means.

(h) Withdraw consent at any time where we are relying on consent to process your personal data if we rely on your consent to process your personal data. You have the right to withdraw that consent at any time.

(i) The right to complain to a supervisory authority in your country of residence. If you believe that our processing of your personal data infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. If you are a resident of an EU or EEA member state, you may do so in the state of your residence. However, the responsible lead supervisory authority for Tibber AS is the Norwegian Data Inspectorate (Datatilsynet) for its cross-border processing activities, in accordance with GDPR Article 56.

If you wish to exercise any of the rights set out above, you can contact Tibber via email at hello@tibber.com.