WHISTLEBLOWER POLICY FASTNED B.V.

1. Introduction

Fastned B.V. ("Fastned") is committed to ensuring that Fastned and its management board and employees act at all times in compliance with all applicable laws and regulations and the Fastned Code of Conduct. Fastned's Whistleblower Policy aims to enable both employees and external parties to speak up when they encounter wrongdoing in the context of their work without the risk of retaliation and with the assurance that all reports are treated confidentially and are promptly investigated. This Whistleblower policy sets out the procedure to be followed to report a breach of the Code of Conduct, internal policies and procedures, laws and regulations.

1.1. Where can this whistleblower policy be found?

Since this policy is targeted at both employees and external (business) partners of Fastned, this policy will be publicly available on www.fastnedcharging.com. Besides, the policy is accessible to all employees of Fastned (Google shared drive 'General') and practical guidance is shared and communicated through training and in quiz form.

1.2. What is the relation to other documents?

The policy must be read in conjunction with the i) Fastned Code of Conduct and the ii) Non-Compliance Response policy. The latter describes the procedure that will be followed to investigate the report after it has been submitted in accordance with this Whistleblower policy.

2. Procedure

2.1 Who can report a concern?

This policy is applicable to anyone who acquired information on breaches in a work-related context with Fastned. These persons can have the status of a worker, (sub-)contractor, supplier, shareholder, member of a supervisory body, (un)paid trainee, etc.

2.2 What types of concerns should be reported under this Whistleblower Policy?

A report of suspected irregularities should be substantive, submitted in good faith and related to one of the following concerns*:*

1. A potential wrongdoing of (European) laws and regulations. In areas such as: anti-money laundering, consumer protection, environmental protection, transport safety and compliance, radiation protection and nuclear safety, public health, public procurement, financial services, protection of privacy, financial interests of the EU, competition law, State aid rules and corporate tax rules;
2. A potential wrongdoing regarding the Fastned Code of Conduct;
3. Conduct that is corrupt, dishonest, or fraudulent;
4. A (potential) danger to the public or employees' health, safety and security or the environment;
5. Theft or fraud against Fastned;
6. Purposeful misinformation or false statements to or by management, to internal or external auditors or public authorities;
7. Inappropriate accounting, financial reporting practices or internal controls;
8. Mismanagement or abuse of authority;
9. Conduct that is detrimental to the interests of Fastned.

Please note that in the case of a fraud incident, the specific procedure described in 4.2 of the Fastned Non-Compliance Response Policy will be followed.

2.3 How can a concern be reported?

Fastned provides an internal reporting channel to report concerns. It is, however, also possible to report to the external channels designated by national authorities (see para. 2.6).

We strongly recommend reporting through the internal reporting channel first before reporting through the external reporting channel. By reporting through the internal reporting channel, the concern can be addressed effectively internally by Fastned itself, allowing Fastned to take immediate measures.

2.4 Internal reporting channels

Should you become aware of any potential breach of laws, regulations, the internal policies and procedures or the Fastned Code of Conduct, you are encouraged to raise this concern in the first instance to your manager. Reporting concerns to management is the fastest and preferred way to address a work-related issue, clear up any misunderstandings, and ensure a good and open work environment.

If this is not possible or appropriate, for whichever reason, please report the breach directly by using the internal reporting channel in order to have your report treated in a confidential manner. You can submit your report in one of the following ways:

E-mail:
whistleblower@fastnedcharging.com

Hotline:
+31 20 809 0365 (24/7 reachable)
Subject to your consent, a complete and accurate written record will be made of your recorded voice message. You will have the opportunity to check this record, correct it and sign it for approval.

Letter:
Attn: Chrissy Schekkerman, Compliance Officer **OR** Hans Bikker, Risk Manager
James Wattstraat 77 R
1097 DL Amsterdam
(Please ensure you indicate CONFIDENTIAL on the envelope)

In person:
Setting up a meeting with our Compliance Officer or our Risk Manager.

- chrissy.schekkerman@fastned.nl (Compliance Officer)
  or
- hans.bikker@fastnedcharging.com (Risk Manager)

The conversation held shall be recorded with your prior consent. Thereafter, a complete and accurate written record will be made of the conversation. You will have the opportunity to check this record, correct it and sign it for approval.

Your report will be received by Fastned's Compliance Officer and/or Risk Manager. These persons are also designated for the follow-up on your report. They are impartial and will maintain contact with you and, where necessary, ask you for further information and provide feedback to you. They will ensure that your identity is not disclosed to others, unless you explicitly authorize this. Emails,

letters, (oral and) written records and all other information provided by you will be securely registered in a dedicated incident file, which will include a date of destroying the file and your confirmation thereof.

2.5 Follow-up

2.5.1 Timeline

Fastned's Compliance Officer or Risk Manager will record the time schedule to be followed in the incident file. If you make yourself known in your report, you will receive acknowledgement of receipt within 7 calendar days (maximum) after the receipt. Within a timeframe of maximum 3 months (following the acknowledgment of receipt) you will be informed about the action envisaged or taken as follow-up to the report and the grounds for the choice of that follow-up.

2.5.2 The investigation of the report

After receipt of your report, Fastned's Compliance Officer or Risk Manager will start a preliminary investigation to verify whether the concern seems prima facie (at first sight) founded. Thereafter, the investigation procedure as set out in the Non-Compliance policy will be followed. This policy also describes which (external) persons will be involved to assess the report, which will depend on the subject of the report. These persons are bound by confidentiality, in accordance with the applicable laws and regulations.

As already stated, only the Compliance Officer and Risk Manager shall have access to your identity. However, in the event that it is evidently impossible to investigate the report if your identity remains unknown to the persons in charge of the investigation, the Compliance Officer and/or Risk Manager may ask you to authorize the disclosure of your identity.

2.6 External reporting channel

In accordance with the EU Directive 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, the EU Member States are under the obligation to designate the authorities competent to receive, give feedback, follow up on reports, and shall provide them with adequate resources. The designated authorities per EU Member State can be found in the national implementation legislation.

The Netherlands
In the Netherlands the following competent authorities will be designated in relation to establishing reporting channels: the Netherlands Authority for Consumers and Markets (ACM), the Netherlands Authority for the Financial Markets (AFM), the Netherlands Data Protection Authority (AP), the Dutch Central Bank (De Nederlandsche Bank N.V.), the House for Whistleblowers, the Inspectorate for Health and Youth Care (IGJ) and the Dutch Healthcare Authority (NZa).

Belgium
At the time of introduction of this policy, Belgium is still in progress of implementing the EU Whistleblower Directive. It is therefore not yet clear which authorities will be designated as the external reporting channels.

Germany
Idem.

France
Idem. However, the Sapin II Law already allows external reporting to judicial authorities, administrative authorities or professional bodies. It should be noted that any person may address

their alert to the French Defender of Rights (Défenseur des Droits) to be directed to the appropriate body competent for receiving the alert.

The United Kingdom
The United Kingdom is under no obligation to implement the EU Whistleblower Directive. In the UK the Public Interest Disclosure Act 1998 ("PIDA") regulates the protection of whistleblowers. PIDA recognises a range of external channels you can make your disclosure to aside from your employer. External disclosures are generally split into two channels, disclosures to:

1. A regulator on the Prescribed Persons list;
2. Anyone else (including a regulator not on the prescribed person list, the police, the press etc).

3. Duty of confidentiality

When you raise a concern, the secrecy of your identity as a whistleblower will be guaranteed in accordance with the applicable laws and regulations.

Your identity will not be disclosed without your explicit consent to anyone beyond the authorized persons competent to receive or follow up on reports (Fastned's Compliance Officer and Risk Manager). This also applies to any other information from which your identity may be (in)directly deduced.

Only if there is a necessary and proportionate obligation imposed by EU or national law in the context of investigations by national authorities or judicial proceedings, your identity might be disclosed, including with a view to safeguarding the rights of defense of the persons concerned.

4. Anonymity

Fastned encourages you to disclose your identity when you report a concern. This way we know who we need to protect (you) and who we can turn to for additional information so that no one is falsely accused on the basis of wrong information.

However, if no other option is feasible, you can report your concern anonymously. This means that even the Compliance Officer and Risk Manager will not know your identity. In that case, you can file your concern by letter. We insist that you indicate **CONFIDENTIAL** on the envelope.

An anonymous report will only be considered valid if it contains enough factual elements to investigate the facts. Therefore, please include as much detail as possible to mitigate difficulties investigating and following up on an anonymous report.

5. Protection of the whistleblower

No member of the personnel of Fastned who reports an event may be sanctioned or subject to any discriminatory measure for having notified an alert selflessly and in good faith via the whistleblowing mechanism.

Fastned does not allow retaliation of any kind against those who, in good faith, report an infringement or suspicion of an infringement of the rules or guidelines. If you report a concern and

it appears that you were genuinely mistaken or if there is an innocent explanation for your concerns, you will not be sanctioned or subject to a discriminatory treatment.

To guarantee this, the Compliance Officer and/or Risk Manager will regularly check in with you during and after the investigation to actively seek your input on whether you feel that there is (risk of) retaliation. If you indicate that you feel retaliated, this will be seriously investigated and remedied if needed.

This assurance does not apply to those who maliciously start an investigation for a matter that is false. While not intending to discourage anyone from reporting matters of genuine concern, it is strongly suggested that you ensure, as far as possible, that a report is factually accurate, complete, from first-hand knowledge, presented in an unbiased fashion (with any possible perception of the whistleblower disclosed), and without material omission. Where it is established that an employee is not acting in good faith or has intentionally made a false report, the employee may be subject to disciplinary measures that may include dismissal.

This Whistleblower Policy was last updated 9 March 2022.