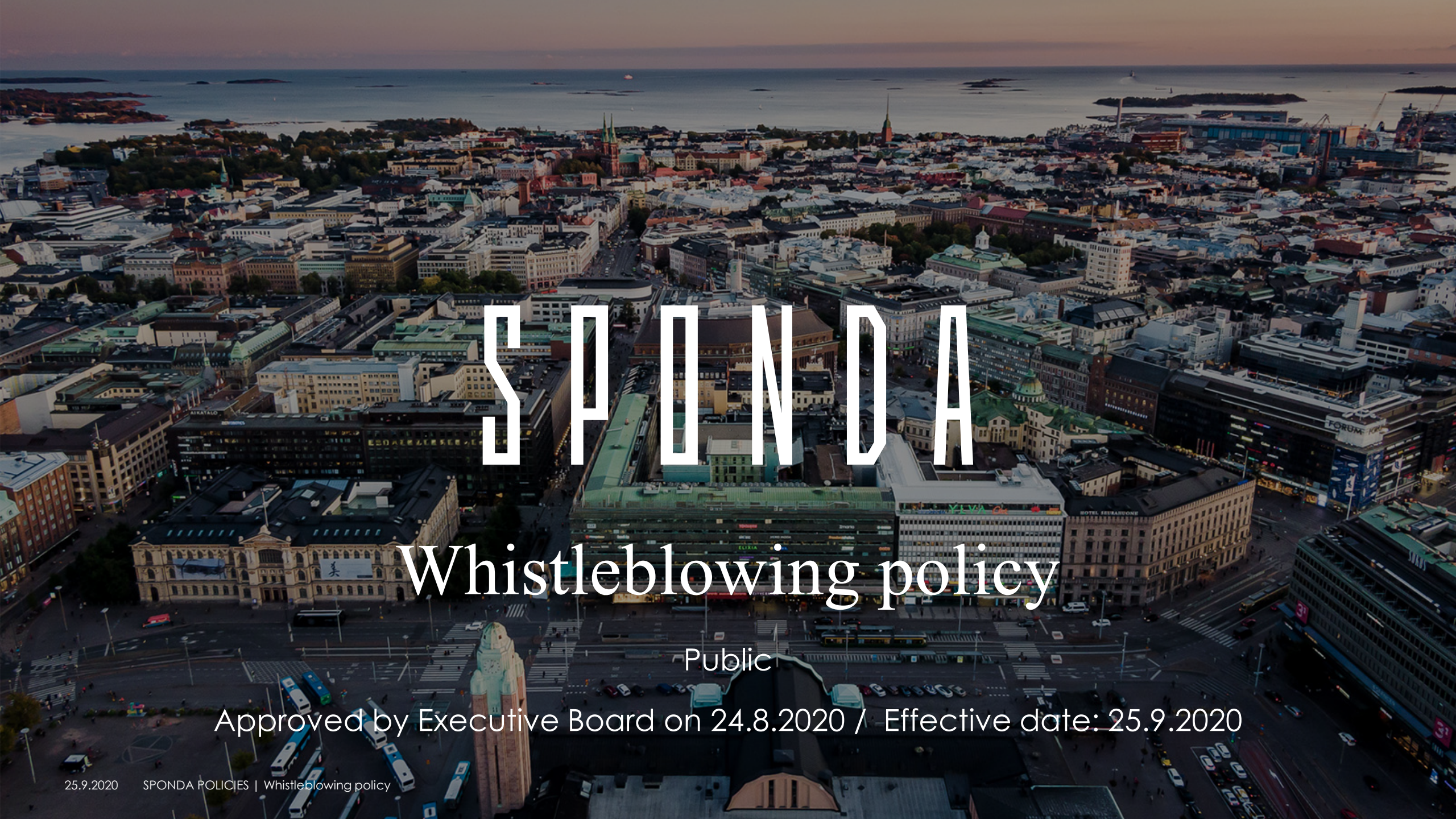

SPONDA

Whistleblowing policy

Public

Approved by Executive Board on 24.8.2020 / Effective date: 25.9.2020

What is whistleblowing and why is it important?

WHAT

This policy lays down the protocols and procedures of **how Whistleblowing cases are handled in Sponda**. Whistleblowers are encouraged to contact their closest contact person or Sponda customer service, but if they feel they cannot, we provide an anonymous whistleblowing channel operated by an external partner, WhistleB. This policy is based on the EU General Data Protection Regulation, EU Directive on Whistleblower Protection and national legislation on whistleblowing.

WHY

We want to succeed by being the best by our own merits. Our business should be conducted in a fair, transparent and ethical way as is described also in our Code of Conduct. If there is an issue, we want to know about it. To achieve this, we want our employees (including temporary workers, trainees and interns), partners and other stakeholders to feel safe to speak up if they notice any unethical or illegal behavior or have questions on the way we operate.

HOW

Cases may be given in person or through an anonymous Whistleblowing Channel. The Whistleblowing Channel offers a possibility to alert the company about suspicions of misconduct in confidence. It is an important tool for reducing risks and maintaining trust in our operations by enabling us to detect and act on possible misconduct at an early stage. The channel is separate from Sponda's technical architecture in order to ensure anonymity and information security. Only Primary Case Handlers have access to the materials within the whistleblowing system. All case documentation is securely saved within the system and nowhere else. The only exception is if the documentation is needed as evidence for official investigations conducted by authorities.

FOR WHOM

Whistleblowing can be done by any person openly or anonymously.

SPONDA

When to blow the whistle?

The whistleblowing channel can be used to alert us about serious risks affecting individuals, our company/organization, the society or the environment.

- The processing may refer to data about serious improprieties concerning:
  - accounting, internal accounting controls, auditing matters, fight against bribery, banking- and financial crime
  - other serious improprieties concerning the company's or the group's vital interests or the life or health of individual persons, as for instance serious environmental crimes, major deficiencies that regard the security at the place of work and very serious forms of discrimination or harassments
  - other illegal action or conflicts of interest
  - serious unethical behavior

- A person who blows the whistle does not need to have firm evidence for expressing a suspicion. However, deliberate reporting of false or malicious information is forbidden. Abuse of the whistleblowing service is a serious disciplinary offence.

- Employees are asked to contact their supervisor or manager for issues relating to dissatisfaction in the workplace or related matters, as these issues cannot be investigated in the cope of the whistleblowing.

- WHISTLEBLOWING CHANNEL MUST NOT BE USED TO REPORT EVENTS PRESENTING AN IMMEDIATE THREAT TO LIFE OR PROPERTY! In such case contact Sponda directly.

How to blow the whistle?

There are different ways to raise a concern:

- ***Alternative 1*** *Contact your closest contact person or Sponda Customer Service directly to report an issue.*

- ***Alternative 2*** *Anonymous and confidential messaging through the Whistleblowing Channel to the whistleblowing team: <https://report.whistleb.com/en/Sponda*

- We encourage anybody who shares their suspicions to be open with their identity. All messages received through either means will be handled confidentially. For those wishing to remain anonymous, we offer a channel for anonymous reporting. The whistleblowing channel enabling anonymous messaging is administrated by WhistleB, an external service provider. All messages are encrypted. To ensure the anonymity of the person sending a message, WhistleB deletes all metadata, including IP addresses. The person sending the message also remains anonymous in the subsequent dialogue with responsible receivers of report.

- An external link to the Whistleblowing Channel is on our website www.sponda.fi on the Code of Conduct page. Internally the link is at the Code of Conduct page in our Intranet. This Whisteblowing Policy and the Privacy Policy are available at both locations.

- **Alternative 3:** Direct reporting to law enforcement or authorities

- **Alternative 4:** Public reporting, if law enforcement agency or competent authorities have failed to take sufficient measure.

SPONDA

The case handling process

1. Primary Case Handlers receive the report
2. Primary Case Handlers acknowledges notifier within 7 days
3. Evaluation and investigation
4. Inform notifier of case status within 3 months
5. Inform notifier when case is closed and of the outcome if possible
6. Analysis and steps to prevent similar events in the future

- Sponda has a standardized case handling process, which has been approved by the Executive Board July 2, 2020.

The case handling process

THE WHISTLEBLOWING TEAM

The Primary Case Handlers together with the persons participating to the investigation process form a **Whistleblowing Team**.

Access to notifications received through our Whistleblowing Channel is restricted to the appointed individuals with the authority to handle whistleblowing cases. At Sponda, the **Primary Case Handers** are the Chief Legal Officer (CLO) and the HR Director. The Audit Committee President will be informed of all notifications and will participate in the handling when needed. The Team's actions are logged and handling is confidential.

When needed, individuals who can add expertise may be included in the investigation process. These people can access relevant data and are also bound to confidentiality.

If a person raises a concern directly to their contact person, Customer Service or by contacting the Primary Case Handers in person the message is also treated according to this policy.

RECEIVING A NOTIFICATION

Upon receiving a notification, the Primary Case Handlers evaluate whether to accept or decline the message. If the message is accepted, appropriate measures for investigation will be taken, please see Investigation below.

The Primary Case Handlers may decline to accept a message if:

- the alleged conduct is not reportable conduct under this Whistleblowing policy
- the message has not been made in good faith or is malicious
- there is insufficient information to allow for further investigation
- the subject of the message has already been solved

If a message includes issues not covered by the scope of this Whistleblowing policy, the Primary Case Handlers should take appropriate actions to get the issue solved.

The Primary Case Handlers will confirm receiving the message within seven (7) days. They will send appropriate feedback of the case status within 3 (or maximum 6 months) upon the date of receiving the report.

Do not include sensitive personal information about anybody mentioned in your message if it is not necessary for describing your concern.

The case handling process

INVESTIGATION

All messages are treated seriously and in accordance with this Whistleblowing policy.

- No one from the Whistleblowing Team will attempt to identify the Whistleblower.
- The Primary Case Handers can, when needed, submit follow-up questions via the channel for anonymous communication.
- A message will not be investigated by anyone who may be involved with or connected to the misgiving.
- The whistleblowing team decides if and how a whistleblowing message should be escalated.
- Whistleblowing messages are handled confidentially by the parties involved.

The Primary Case Handers will assign the case a tier and a Whistleblowing Team based on the seriousness and the nature of the case.
The Whistleblowing Team will then take the appropriate steps to investigate the case and decide on the necessary steps.

CLOSING THE CASE

Once the case has been investigated, needed steps for correction are taken and the case is evaluated for possible future development needs.
The Whistleblowing Team will then write a Case Report to be filed in the Whistleblowing Channel archive.

Any other case materials are evaluated for archiving purposes, any personal information is redacted from materials that are archived within the whistleblowing channel. Unnecessary materials are destroyed.

Whistleblower protection

WHISTLEBLOWER PROTECTION IN THE CASE OF NON-ANONYMOUS WHISTLEBLOWING

A person expressing genuine suspicion or misgiving according to this policy will not be at risk of losing their job or suffering any form sanctions or personal disadvantages as a result. It does not matter if the whistleblower is mistaken, provided that he or she is acting in good faith.

Subject to considerations of the privacy of those against whom allegations have been made, and any other issues of confidentiality, a non-anonymous whistleblower will be kept informed of the outcomes of the investigation into the allegations.

In cases of alleged criminal offences, the whistleblower will be informed that his/her identity may need to be disclosed during judicial proceedings.

PERSONAL DATA

Data is stored within the EU. There is a general prohibition on the transfer of personal data out of the European Economic Area (EEA) unless specific mechanisms are used to protect data.

PROTECTION OF, AND INFORMATION TO, A PERSON SPECIFIED IN A WHISTLEBLOWER MESSAGE

The rights of the individuals submitting the message or specified in a whistleblower message are subject to the relevant data protection laws. Those affected will be entitled to the right to access data relating to themselves and should the information be incorrect, incomplete or out of date to require amendments or deletion of data.

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.

DELETION OF PERSONAL DATA

Personal data included in a whistleblowing messages and investigation documentation is deleted when the investigation is complete, with the exception of when personal data must be maintained according to other applicable laws. Permanent deletion is carried out 30 days after completion of the investigation. Investigation documentation and whistleblower messages that are archived should be anonymized under GDPR; they should not include personal data through which persons can be directly or indirectly identified.

SPONDA

For more information

Anonymous WhistleB reporting service »

Code of Conduct and Whistleblowing Policy on the Sponda webpage »

In cases of immediate danger to life or property, contact Sponda directly »

Please contact us, if you are unsure if an issue should be reported or not, if you want to report an issue personally or have any other questions about this policy:

Sponda Ltd
Customer Service Center
+358 20 355 6677, on weekdays at 8.00–16.00
Email: customerservice@sponda.fi

Change history

Date	Issue
24.8.2020	Whistleblowing policy created and approved by Executive Board.