Date 30.11.2023

Technopolis whistleblowing guidelines

1. Introduction – what is whistleblowing, and why is it important?

Our organisation strives to achieve transparency and a high level of business ethics. Our whistleblowing channels operated under these guidelines (the "**whistleblowing service**") offers a possibility to alert the organisation about suspicions of misconduct in a confidential way. We encourage all our employees to use these services as described in these guidelines. 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. Whistleblowing can be done openly or anonymously.

The protection of the whistleblower is determined in accordance with applicable laws in particular the national legislation implementing the EU Whistleblower Protection Directive (2019/1937) as well as other applicable national whistleblowing legislation.

2. When to blow the whistle?

The whistleblowing service can be used to alert us about serious risks of wrongdoing affecting people, our organisation, the society or the environment.

Reported issues include criminal offences, irregularities, and violations or other actions in breach of EU or national laws within a work-related context, for example:

- ✓ **Corruption and financial irregularities**; for example, bribes, unfair competition, money laundering, financing of terrorism, fraud, conflict of interest, public procurement violations
- ✓ **Health and safety violations**; for example, product safety and compliance, traffic and transport safety, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health
- ✓ **Consumer protection**
- ✓ **Public procurement** with the exception of defence and security procurement
- ✓ **Environmental protection violations**; for example, illegal treatment of hazardous waste
- ✓ **Privacy and cyber security violations**; for example, improper use of personal data, hacking

Employees are asked to contact their supervisor or manager for issues relating to dissatisfaction in the workplace, harassment or bullying or related employment matters, as these issues cannot be investigated in the scope of whistleblowing service. Special provisions apply for whistleblowing service in certain jurisdictions, see below. Further, please note that our whistleblowing service should not be used for general customer feedback.

It is stated for the sake of clarity that the national laws implementing the Whistleblower Protection Directive (2019/1937) apply only to the breaches of certain specified legislation and regulations. Detailed scope is defined in each applicable national law.

- The applicable law in Finland is the Act on the protection of persons reporting violations of European Union and national law 1171/2022, as amended (in Finnish: *laki Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta*).
- The applicable statutory framework in Sweden, see the next section.
- The applicable statutory framework in Norway is the Norwegian Working Environment Act (in Norwegian: *Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven), LOV-2005-06-17-62*), as amended, which includes provisions regarding whistleblowing in chapter 2 A Notification.

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.

Please see below under this section 2 certain jurisdiction specific guidance on whistleblowing which is applied before the above in the respective jurisdiction. In other jurisdiction covered by these guidelines the above guidance applies.

WHISTLEBLOWING SERVICE IN SWEDEN

Technopolis entities in Sweden have established a whistleblowing reporting channel. In this whistleblowing channel, we can only handle reports about suspected serious misconduct involving persons in key or leading positions within the Technopolis Swedish business' or Technopolis group. The term "serious misconduct" refers to serious irregularities relating to:

- ✓ accounting, internal accounting controls and/or auditing matters,
- ✓ bribery and corruption,
- ✓ money laundering,
- ✓ the life or health of individual persons (e.g., serious environmental crimes, major deficiencies as regards the security at the place of work and very serious forms of discrimination or harassments), or
- ✓ vital interests of the Technopolis Swedish business or group.

Due to the statutory restrictions, only reports of the above character may be submitted in the whistleblowing reporting channel in Sweden. If the report does not fall within the scope of the whistleblowing channel in Sweden, it may be processed in another handling process subject to applicable statutory requirements.

However, all individuals are always encouraged to provide reports concerning also other suspected misconduct than the mentioned above. All other reports that do not relate to the issues above shall be brought up directly with for example one's manager or Technopolis HR or Technopolis Group CEO, as

appropriate taking into account the subject of the report. Alerts of all such matters belonging to the scope of the whistleblowing policy shall be reported directly to the whistleblowing channel.

WHISTLEBLOWING SERVICE IN NORWAY

According to the Norwegian Working Environment Act (WEA), an employee (including temporary employee hired through temp agency) has a right to report issues of concern which include breaches of legislation, written ethical guidelines in the undertaking or ethical norms on which there is broad agreement in society, for example, circumstances that may involve: (i) danger to life or health, (ii) danger to climate and the environment, (iii) corruption or other economic crime, (iv) abuse of authority, (v) unsatisfactory working environment, and (vi) breach of personal data security. Matters raised that only relate to the employee's work situation shall not be considered whistleblowing according to WEA unless the matter also involves issues of concern as described above.

In Norway in addition to using our whistleblowing service an employee may always report issues of concern internally to the employer, a representative of the employer, in accordance with these whistleblowing routines via a safety representative, union representative or lawyer. An employee may also always report issues of concern externally to a public supervisory authority or other public authority.

3. How to blow the whistle in our whistleblowing service?

You can file anonymous or confidential messaging through the whistleblower reporting channel to the whistleblowing team as follows:

In Finland: https://report.whistleb.com/technopolisfinland

In Sweden: https://report.whistleb.com/technopolissweden

In Norway: https://report.whistleb.com/technopolisnorway

All messages received will be handled confidentially. The whistleblowing channel 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 meta data, including IP addresses. The person sending the message also remains anonymous in the subsequent dialogue with responsible receivers of the report.

4. Investigation process

THE WHISTLEBLOWING TEAM

Access to messages received through our whistleblowing channel as well as to other investigation material is restricted to appointed individuals with the authority to handle whistleblowing cases. Their actions are logged and handling is confidential. When needed, individuals who can add expertise may be included in the investigation process in accordance with requirements under applicable law. These individuals can access relevant data and are also bound to confidentiality.

The whistleblowing team consists of: Outi Raekivi, Olli Rautiainen and Risto Kivisilta.

RECEIVING A MESSAGE

Upon receiving a message, the whistleblowing team decides whether to accept or decline the message. If the message is accepted, appropriate measures for investigation will be taken, please see Investigation below.

The whistleblower will receive an acknowledgment of receipt of the report within 7 days.

The whistleblowing team may not investigate the reported misconduct if:

- ✓ the alleged conduct is not reportable conduct under these Whistleblowing guidelines
- ✓ 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 these Whistleblowing guidelines, the whistleblowing team should provide the reporting person with appropriate instructions.

The whistleblowing team will send appropriate feedback within 3 months upon the date of receiving the report, however, taking into consideration possible statutory restrictions.

INVESTIGATION

All messages are treated seriously and in accordance with these Whistleblowing guidelines.

- ✓ The whistleblowing team can, when needed, submit follow-up questions via the channel for anonymous communication and obtain relevant information for the investigation from other sources.
- ✓ A message will not be investigated by anyone who may be involved with or connected to the wrongdoing.
- ✓ Whistleblowing messages are handled confidentially by the parties involved.
- ✓ Corporate or external expertise may be included in the investigation in accordance with requirements under applicable law.

5. Protection and privacy

WHISTLEBLOWER PROTECTION

A person expressing genuine suspicion or misgiving according to these guidelines will not be at risk of losing their job or suffering any form of 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. However, please note that applicable laws may vary between the countries where we operate. If you have further questions on the protection of whistleblower, please contact the whistleblowing team.

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

Information regarding an identity of a whistleblower and other persons involved in a whistleblowing matter shall be treated with confidentiality and may not be unauthorizedly disclosed to anyone outside the

whistleblowing team. Information may be disclosed in order to fulfil a legal obligation, notify competent authorities, during a judicial proceeding or if a disclosure of the information is otherwise required or permitted under applicable law.

PROCESSING OF PERSONAL DATA

We may collect personal data on the person specified in a message, a whistleblower submitting the message and any third person involved in the investigation. The processing is based on statutory obligations and legitimate interests as described in our privacy policy as in force from time to time.

You may exercise your legal rights as a data subject in accordance with the local data protection legislation such as right of access, of rectification and of opposition, as well as of limited processing of your personal data. These rights may be subject to possible overriding safeguarding measures required to prevent the destruction of evidence or other obstructions to the processing and investigation of the case.

Further information on processing of personal data, including the legal basis for processing, purposes of the processing and legal rights of the data subject, is available in our privacy policy as in force from time to time. The most current version of the privacy policy can be found here: https://technopolisglobal.com/privacy-policy/whistleblowing-service-register.

RETENTION OF DATA

Different countries have differing rules on how long personal data gathered from the whistleblowing reports may be processed. We do not store personal data longer than provided for in the applicable national legislation and necessary for the purposes outlined in our privacy policy. The storage period depends on the nature of the information and on the purposes of processing. The maximum period may therefore vary per use.

Personal data included in a whistleblowing messages and investigation documentation is deleted when the investigation is complete, with the exception of when personal data may be maintained according to the applicable laws. Permanent deletion from the whistleblowing service is carried out 30 days after completion of the investigation, however, the reported data may be retained thereafter outside the service in accordance with these guidelines.

In Finland and Norway, the data retention period is as a rule five (5) years from the when the whistleblowing case was received by the controller or its group company. In Sweden, the data retention period is as a rule two (2) years from the date when the whistleblowing case is closed. However, the data will not be retained longer than is necessary for the purposes of processing.

PERSONAL DATA CONTROLLERS

Technopolis Holding Oyj is the main data controller in respect of any personal data reported within the whistleblowing service. In addition, our local country-specific company to which the specific whistleblowing case relates may also be data controller or joint controller under applicable data protection laws. See more information in our privacy policy.

PERSONAL DATA PROCESSORS

WhistleB Whistleblowing Centre Ab (World Trade Centre, Klarabergsviadukten 70, SE-107 24 Stockholm) is responsible for the whistleblowing application, including processing of encrypted data, such as

whistleblowing messages. Neither WhistleB nor any sub-suppliers can decrypt and read messages. As such, neither WhistleB nor its sub-processors have access to readable content.

More information on the data processors, see our privacy policy.

6. External reporting

Our whistleblowing service is the primary reporting channel. However, under applicable law you may have the right in certain exceptional situations to report an issue to an external whistleblower channel provided by a competent authority in each jurisdiction.

Please see Annex 1 for country-specific external whistleblowing bodies.

Appendix 1: External whistleblowing bodies

EXTERNAL REPORTING CHANNEL IN FINLAND

The competent authority in Finland is the Office of the Chancellor of Justice (*in Finnish: Oikeuskanslerin virasto*). Complaint to the competent authority can be made by email or by regular mail, or verbally or using electronic reporting platform. For further information and instructions, please see links below:

In English: https://oikeuskansleri.fi/en/about-whistleblower-protection

In Finnish: https://oikeuskansleri.fi/tietoa-ilmoittajansuojelusta

EXTERNAL REPORTING CHANNELS IN SWEDEN

In Sweden, the reporting should be made using the relevant authority's established reporting channels designated for reporting of wrongdoings. Which competent authority should handle the report depends on the nature of the alleged wrongdoing. The appointed competent authorities in Sweden are listed below.

Swedish Authority	Access to whistleblowing channel
Work Environment Authority	Reports concerning certain product security (relating to e.g. protective equipment and machines), as well as all misconduct that is not covered by any other authority's area of responsibility https://www.av.se/om-oss/visselblasarlagen/extern-rapporteringskanal/?hl=rapporteringskanal
National Board of Housing, Building and Planning	Reports concerning product security relating to construction https://www.boverket.se/sv/om-boverket/visselblasning/
Safe and interference-free electricity	Reports concerning certain product security relating to electrical safety https://www.elsakerhetsverket.se/yrkespersoner/tillverka-och-salja-elprodukter/sla-larm-om-missforhallanden/
Economic Crime Authority	Reports concerning EU's financial interests, such as EU fraud and certain VAT fraud https://www.ekobrottsmyndigheten.se/visselblasarfunktion-eu-medel/
Estate Agents Inspectorate	Reports concerning financial services, products and markets or money laundering and finance of terrorism with connections to the real estate market https://fmi.se/det-har-ar-fmi/kontakta-oss/visselblasning-om-penningtvatt-eller-finansiering-av-terrorism/
Financial Supervisory Authority	Reports concerning certain financial services, products and markets or money laundering and finance of terrorism within the financial market https://www.fi.se/sv/om-fi/kontakta-oss/visselblasare/
Public Health Agency	Reports concerning certain product security (relating to e.g. tobacco) and certain public health issues https://www.folkhalsomyndigheten.se/livsvillkor-levnadsvanor/andts/regler-for-tillverkning-handel-och-hantering/visselblasning-tobaksomradet/
Agency for Marine and Water Management	Reports concerning environmental protection relating to ocean, lakes or watercourses https://www.havochvatten.se/om-oss-kontakt-och-karriar/om-oss/visselblasarfunktion.html
Authority for Privacy Protection	Reports concerning data protection and breaches of GDPR https://www.imy.se/privatperson/utfora-arenden/visselblasning/
Inspectorate of Strategic Products	Reports concerning product security relating to dual-use items or military equipment https://isp.se/om-isp/visselblasning-till-isp/hur-rapportering-ska-ske/

Health and Social Care Inspectorate	Reports concerning certain public health issues (relating to e.g. blood- and transplant operations) https://www.ivo.se/om-ivo/kontakta-oss/visselblasning/
Chemicals Agency	Reports concerning certain product security and environmental protection relating to chemical legislation https://www.kemi.se/om-kemikalieinspektionen/kontakta-oss/extern-kanal-for-visselblasning
Consumer Agency	Reports concerning certain product security, public health or consumer protection issues https://www.konsumentverket.se/om-konsumentverket/var-verksamhet/visselblasning/extern-kanal-for-visselblasning/
Competition Authority	Reports concerning public procurement or competition on the EU market https://www.konkurrensverket.se/tipsa-oss/visselblasarfunktion/
Food Agency	Reports concerning certain product security, environmental protection, food safety and animal well-being https://www.livsmedelsverket.se/om-oss/kontakt/visselblasning--rapportera-om-missforhallanden
Medical Products Agency	Reports concerning certain product security or public health issues relating to pharmaceutical https://www.lakemedelsverket.se/sv/om-lakemedelsverket/kontakta-oss/visselblasning
County Administrative Boards	Reports concerning certain product security and environmental protection. For information on how to report to a county, please visit the relevant county's website on www.lansstyrelsen.se
Civil Contingencies Agency	Reports concerning certain product security, relating to e.g. pyrotechnical products and explosives used for civil purposes https://www.msb.se/sv/om-msb/kontakta-oss/visselblasning--rapportera--om-missforhallanden/visselblasning--rapportera--om-missforhallanden-inom-omradet-produktsakerhet-och-produktoverensstammelse/
Environmental Protection Agency	Reports concerning certain product security and environmental protection (such as emissions trading) https://www.naturvardsverket.se/om-oss/kontakt/visselblasning/rapportera-missforhallanden-inom-vissa-tillsynsomraden/
Post and Telecom Authority	Reports concerning certain product security and safety relating to network- and information systems and certain data privacy issues within electronic communication https://www.pts.se/sv/om-pts/visselblasning/
Government Offices of Sweden	Reports relating to state aid https://www.regeringen.se/om-webbplatsen/rapportera-missforhallanden-om-statsstod/
Inspectorate of Auditors	Reports concerning financial services, products and markets or money laundering and finance of terrorism relating to auditor requirements https://www.revisorsinspektionen.se/tillsyn/rapportering-om-missforhallanden/
Tax Agency	Certain reports relating to taxes https://www.skatteverket.se/omoss/varverksamhet/styrningochuppfoljning/skattekontroller/rapporteraommissforhallandeninomskatteomradet.4.1df9c71e181083ce6f636e5.html
Forest Agency	Reports concerning certain product security and environmental protection relating to forestry https://www.skogsstyrelsen.se/kontakt/visselblasarfunktion/
Board of Agriculture	Reports concerning e.g. animal health and well-being, animal protection, animal food and ecological production https://jordbruksverket.se/om-jordbruksverket/visselblasarfunktion-for-offentliga-kontroller
Energy Agency	Reports concerning certain product security or safety relating to network- and information systems https://report.whistleb.com/sv/Energimyndigheten

Radiation Safety Authority	Reports relating to radiation protection and nuclear safety https://www.stralsakerhetsmyndigheten.se/kontakt/visselblasarfunktion/
SWEDAC (Sweden's national accreditation body)	Reports concerning certain product security https://www.swedac.se/visselblasning/#_ftn1
Gambling Authority	Reports concerning financial services, products and markets or money laundering and finance of terrorism relating to gambling companies https://www.spelinspektionen.se/lagar--forordningar/penningtvatt/visselblasarfunktion/
Transport Agency	Reports concerning certain product security or transport security https://www.transportstyrelsen.se/sv/Omtransportstyrelsen/Vill-duanmala-misstankar-omkorruption-mutor-eller-jav/

EXTERNAL REPORTING CHANNEL IN NORWAY

An employee may notify externally to a public supervisory authority or other public authority such as the Norwegian Labour Authority. Please see below some examples of authorities' communication channels where a notification may be made:

Labour Authority (Arbeidstilsynet) on
https://tips.arbeidstilsynet.no/skjema/steg1-1

Tax authorities (Skatteetaten) on
https://www.skatteetaten.no/tipsoss/

Social Security office (NAV) on
https://www.nav.no/samarbeidspartner/trygdesvindel

Economic Crime Authority (Økokrim) on
https://www.okokrim.no/tips-oss-generelt.565708.no.html

Financial Supervisory Authority (Finanstilsynet) on
https://www.finanstilsynet.no/om-finanstilsynet/varsling-til-finanstilsynet/

Authority for Privacy Protection (Datatilsynet) on
https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/klage-til-datatilsynet/