Group Whistleblowing Policy

Document Owner	General Counsel
Approval	Board of Directors of Olink Holding AB (publ) (the “Company” and together with its subsidiaries the “Group” or “Olink”)
Date of Approval	25 February 2021
Effective as of	The Effective Date of the Company’s Registration Statement on Form F-1

Contents

1. Introduction

1.1 Purpose

Conducting business responsibly, with integrity and transparency is one of the core foundations of our business. This is reflected in our core values. Illegal or dishonest activities as well as other wrongdoings hinder economic growth by confounding market principles, and the victims are individuals and businesses that rely on sustainable growth for their physical and social well-being. A comprehensive framework of well-defined policies, procedures and standards is required to facilitate and ensure the core foundations of our business.

The Company shall take appropriate action when wrongdoing happens. To ensure this, knowledge of any wrongdoing is of highest importance. The Company therefore promotes a culture where employees feel safe and are encouraged to act and report any wrongdoing related to our operations.

This Whistleblowing Policy (this "**Policy**") is an essential part of this commitment. It ensures that anyone working for the Company can report any wrongdoing. It also provides protection to any individual making a report of potential misconduct. In short, the purpose and meaning of this Policy is to:

- protect whistleblowers from retaliation;
- protect the reasonable interests of those accused;
- establish requirements to safeguard confidentiality and anonymity including ensuring personal data law compliance; and
- establish procedures for reporting and for the handling of reports or wrongdoings.

1.2 Implementation and scope of application

The Document Owner is responsible for ensuring that this Policy is implemented and monitored throughout the Group and that trainings are held at least on a yearly basis. This Policy is owned by the Document Owner specified in Section 2 below and shall be reviewed at least annually for required updates. As business and regulatory requirements constantly change, it is critical for the Document Owner to ensure that this Policy is updated regularly as needed and that a strong interface to the business functions of the Company exists.

This Policy applies to the operations and all employees of the entire Group, including members of management and the Board of Directors (all of whom are included in the term "employee" for purposes of this Policy). Adherence to this Policy is both an individual and corporate responsibility. In particular, it is the responsibility of the managers with staff supervisory responsibility to ensure that employees and consultants are informed of this Policy. In addition, recruiting managers shall ensure that any new employee or consultant is informed of this Policy.

Any requests for exceptions to this Policy must be documented in writing by the relevant business unit, clearly defined, include a plan for how and when to comply, and be approved by the Document Owner. Exceptions shall be time limited.

2. Roles and Responsibilities

Roles	Responsibilities
The Board of Directors	• Approves this policy and changes thereto.
Group CEO & Management	• Responsible for commercial risk assessment and overall accountable for following up on wrongdoings within the Group. • Report to the Board of Directors of the Group. •
General Counsel	• Operational responsibility for this Policy and the implementation hereof. • Responsible for selection and supervision of system support for whistleblowing. • Overall responsibility for review of the management of reported wrongdoings (responsibility for managing investigations and actions upon wrongdoings will reside with head of entities/business areas). • Responsible for trainings regarding this Policy. • Responsible for performing regular assessment to measure implementation status of this Policy and support business areas with guidance to improve maturity based on the business needs and risk exposures. • Report general risk assessment, implementation updates and specific high-risk situations to the Enterprise Risk Manager and the Group CEO.

Head of entities/business areas	• Be aware of potential risks of wrongdoings identified within their respective business areas. • Identify, assess, manage and escalate risks of or wrongdoings in their respective areas. • Record any occurrence and consequence of a risk of or wrongdoing that has been reported under this Policy. • Escalate and report identified risks and wrongdoings to the General Counsel.
Managers with staff or recruitment responsibility	• Introduce and provide information about this Policy to new employees and information on updates to this Policy to all employees.
Employees	• Each employee has a responsibility to follow this Policy and its underpinning guidelines and instructions.

3. What Activities Should Be Reported

3.1 All wrongdoings should be reported. "Wrongdoings" means illegal or dishonest activities such as, but not limited to, violations of law, harassments, violations of the Group's policies, such as the FCPA and Anti-Corruption Policy, irregular activities in accounting and book-keeping, the internal control of accounting and book-keeping, audits and combating bribery, the lives and health of natural persons, damage to the environment as well as other irregularities that concern the Group's vital interests.

3.2 The whistleblower must exercise sound judgement to avoid baseless allegations.

4. How to Report Wrongdoings

4.1 It is important for the Group that employees, representatives or other persons acting on behalf of the Group help discover wrongdoings by reporting such wrongdoings. The Group has therefore implemented low-threshold possibilities for reporting any wrongdoing. All whistleblowing channels are designed, set up and operated in a way that ensures the confidentiality of the whistleblower.

4.2 Reports of wrongdoings may be reported to the:

- Legal Department; or
- Directly to the manager of the individual employee.

4.3 This policy applies to all wrongdoings and thus to any person suspected of such wrongdoing. Due to personal data legislation, the Group may however, as a general rule, not digitally process all information relating to a person's criminal convictions or offences or suspicion that a person has committed criminal offences. Concerns may be submitted digitally via e-mail or through the Company-designated whistleblowing system if the person suspected of wrongdoings holds a key or leading position in the Group. In practice, this means that only wrongdoings by the Group's board of directors, executive management, or representatives of other key business functions may be reported digitally. To report a concern through the Group's whistleblowing system please visit www.whistleblowerservices.com/olink. Any concerns of wrongdoings for other persons than those holding a key or leading position in the Group should only be reported face-to-face, by phone at 1-877-824-3363 or by submitting a printed report.

4.4 Reports may be submitted anonymously. However, if reports are submitted anonymously, the Group or the external investigator may be unable to follow up on the report.

5. How Will a Concern Be Handled

5.1 The Group is committed to listening to employees, learning lessons and improving operations and the work environment. A thorough and proportionate investigation of the whistleblower's report will be carried out by us or by an external party. The person receiving your report shall always write down the date of the report and its main content. The investigation will be objective and evidence-based and will produce a report that focuses on identifying and rectifying any issues and learning lessons to prevent problems from reoccurring.

5.2 Employees who commit wrongdoings may be subject to disciplinary action, up to and including dismissal, depending on facts and circumstances. This Policy does not regulate other potential sanctions which could arise under law.

5.3 Unless the person suspected of wrongdoing holds a key or leading position in the Group, the investigation of the whistleblower's report will be conducted manually and all communication will be held by phone or by post.

6. Whistleblowing Protection

6.1 Whistleblower protections are provided in two important areas – confidentiality and against retaliation.

6.2 Insofar as possible, the confidentiality of the whistleblower will be maintained. However, identity may have to be disclosed to conduct a thorough investigation, to comply with the law and to provide accused individuals their legal rights of defence.

6.3 The Company will not retaliate against a whistleblower. This includes, but is not limited to, protection from retaliation in the form of an adverse employment action such as termination, compensation decreases, or poor work assignments and threats of physical harm. Any whistleblower who believes he/she is being retaliated against must contact the Human Resources department immediately. The right of a whistleblower to protection against retaliation does not include immunity for any personal wrongdoing that is alleged and investigated.

7. Personal Data

7.1 All personal data will be processed in accordance with the General Data Protection Regulation (the "**GDPR**") and all complementary data protection legislation as well as the Group's Personal Data Processing Policy. Details of the processing are set out in Appendix 1 to this Policy.

8. Revision

8.1 The Group's Chief Executive Officer is ultimately accountable for this Policy, but it resides with the General Counsel. The General Counsel is responsible for its documentation and updates.

8.2 This Policy shall be reviewed at least annually by the General Counsel, or if the objectives within the instruction have changed Any significant changes to the document are subject to approval by the Board of Directors.

9. Further Guidance and Assistance

9.1 This Policy is the fundamental policy document. It sets forth the framework for the Group's compliance with rules and principles. Each employee is responsible for knowing which policies, directives and related documents apply to them.

9.2 For questions regarding this policy, please contact the Document Owner.

* * * *

APPENDIX 1 – PROCESSING OF PERSONAL DATA

Reports made in accordance with this Policy are likely to contain personal data pertaining to the person who has made the notification, and/or to the person suspected of the alleged wrongdoing. The types of personal data which may be processed in conjunction with an investigation are typically the following:

- The name, position, and contact details of the employee who submitted the complaint and the individual to whom the complaint relates, as well as any witnesses or other individuals affected.

- Details of the misconduct of which the person reported is suspected (including data relating to criminal acts or sanctions, to the extent permitted by applicable law).

The Company is the data controller of any personal data collected via the whistleblowing system, and thereby responsible for ensuring that such data is processed in accordance with applicable law. In case of questions related to personal data processing, please contact a member of the Company's Legal Department, or the Company's Data Protection Officer.

Personal data will be processed only to the extent required to investigate a concern and by a restricted number of individuals at the Company who are involved in the investigation. In this context, personal data may be transferred to a department within the Company (such as internal audit, if applicable), executive management, the board of directors, or other persons closely related to the Company. In addition, personal data may be transferred to the police or other law enforcement authorities, forensic companies, or independent auditors. To the extent deemed necessary, it may also be transferred to the Company's affiliates. If it is necessary to transfer personal data to individuals or companies in countries outside the EU/EEA, the Company will ensure that there is a legal basis for such transfer and that the transfer is safeguarded as required by the GDPR, e.g. by including the standard contractual clauses adopted by the EU Commission (which are available at the EU Commission's website) in the agreement with the receiving party located outside of the EU/EEA.

Personal data will not be retained longer than is necessary. Complaints, reports, and information regarding misconduct which have been investigated but not resulted in any action will be deleted within two months of the conclusion of the investigation. If it is decided that no investigation will be initiated, the information will be deleted within two months after such decision has been made. If the investigation results in any action being taken against the individual who has been reported, the information will be deleted when the information is no longer needed for the purpose of carrying out an investigation, taking action or to follow up such action.

Note that the person who is reported is entitled to receive information about the report. If it is not possible to inform the individual immediately, for example if such information could jeopardize the Company's investigation, information will be provided at a point of time where it would no longer constitute a risk to the investigation.
When the Company processes personal data, the individual whose data is being processed has rights under applicable law, including the right to (i) request access to (incl. a copy of) his/her personal data undergoing processing and (ii) request rectification or erasure of his/her personal data. The individual is also entitled to object to the processing and lodge a complaint with the supervisory authority