**INTERNAL PROCEDURE FOR HANDLING INTERNAL REPORTS AND TAKING FOLLOW-UP ACTIONS AT FINEJAS IN WROCŁAW**

**§ 1. GENERAL PROVISIONS**

1. In accordance with the obligations set forth in 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, and the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws 2024, item 928), this procedure for handling internal reports and taking follow-up actions is established.
2. The purpose of this procedure is to establish the rules for receiving whistleblower reports, verifying them, and taking explanatory and follow-up actions.
3. This procedure defines:
* established channels for submitting internal reports;
* the procedure for submitting internal reports;
* the organizational unit or external entity authorized to receive internal reports;
* the organizational unit within the structure of the Entity authorized to take follow-up actions, including verifying the internal report and further communication with the whistleblower;
* the conditions for whistleblower protection, including persons assisting in the report, in connection with the submitted report, and the issue of taking follow-up actions;
* the conditions for maintaining a record of reports;
* the principles of personal data processing;
* the means of protecting whistleblowers and persons assisting in the report from retaliatory actions.
1. In connection with the adoption of this procedure, the following definitions are established:
* **Information about a breach of law** – information, including justified suspicion, concerning an existing or potential breach of law that has occurred or is likely to occur within the Entity, in which the whistleblower participated in the recruitment process or other negotiations preceding the conclusion of the agreement, works or worked, or in another legal entity with which the whistleblower has or had contact in the work-related context, or information concerning the attempt to conceal such a breach of law;
* **Reporting channel** – a secure and confidential method established by the Entity for submitting internal reports;
* **Procedure** – this procedure for receiving reports and taking follow-up actions;
* **Entity** – Finejas Poland Sp. z o.o., branch in Białystok, ul. Warszawska 6/32, 15-063 Białystok, NIP 9662138529, REGON: 381368762-00010;
* **Whistleblower** – a natural person who reports or publicly discloses information about a breach of law obtained in a work-related context within the Entity, including an employee, temporary worker, person performing work on a civil contract basis, entrepreneur, proxy, shareholder, or member of the body of a legal person or organizational unit without legal personality, or a person performing work under the supervision and direction of a contractor, subcontractor, or supplier, including under a civil contract, intern, volunteer, trainee, officer as defined by Article 1(1) of the Act of 18 February 1994 on the Pension Provision of Officers of the Police, Internal Security Agency, and other services, as well as those who obtained information in the work-related context before entering into an employment relationship or other legal relationship forming the basis for the provision of work or services, or serving the legal entity;
* **Public disclosure** – making information about a breach of law publicly available;
* **Authorized person** – a person authorized within the structure of the Entity to receive reports, take follow-up actions, including verifying the report, further communication with the whistleblower, and providing feedback to the whistleblower;
* **Report** – information provided to the Entity by the whistleblower concerning information about a breach of law;
* **External report** – information provided by the whistleblower to the Commissioner for Human Rights or a public authority concerning information about a breach of law.

**§ 2. REPORTING CHANNELS**

1. To submit an internal report, the whistleblower shall use the following established reporting channel:
* email address confidentia@finejas.wroclaw.pl to which only the Authorized Person has access.
1. Reports submitted bypassing the established Reporting Channel shall not be considered under the rules outlined in the Procedure.
2. The established Reporting Channel does not apply to external reports, which the whistleblower may submit to the Commissioner for Human Rights or a public authority starting from 25 December 2024. In certain cases, it may be transferred to relevant institutions, bodies, or organizational units of the European Union.
3. The submission of an internal or external report is free of charge.

**§ 3. PROCEDURE FOR SUBMITTING INTERNAL REPORTS**

1. To expedite the processing of the report and the taking of appropriate follow-up actions, it is recommended that the report include:
* the whistleblower's details and method of contact (unless the report is submitted anonymously);
* the details of the person to whom the report pertains;
* the category of the breach of law;
* any circumstances indicating a breach of law;
* information, documents, and other evidence regarding the occurrence of the breach of law or irregularities indicated in the report, particularly data of witnesses of the breach;
* the place, time, and period during which the breach occurred.
1. The whistleblower should familiarize themselves with this Procedure and the information clause on the processing of personal data, which is attached as Appendix No. 1 to this Procedure, before submitting the report.
2. The Entity processes anonymous reports. To submit an anonymous report, it is recommended that the whistleblower uses an email address that does not contain personal data, such as name, surname, or other data that may reveal their identity. It is recommended that the subject and/or content of the report indicate its anonymous nature, and no personal data should be provided.
3. The whistleblower's personal data, which may reveal their identity, will not be disclosed to unauthorized persons unless the whistleblower explicitly consents.
4. If the disclosure of the whistleblower's identity is necessary and proportionate under legal obligations in connection with investigations conducted by public authorities or preparatory or judicial proceedings conducted by courts, the whistleblower will be notified of this before the disclosure. This notification will include an explanation of the reasons for the disclosure unless such notification jeopardizes the investigation or proceedings.
5. To review the report and take explanatory and follow-up actions, the whistleblower may need to provide additional information. In such cases, the Authorized Person has the right to contact the whistleblower to request the necessary details.
6. In the case of an anonymous report, the Authorized Person will not provide the information required by this Procedure unless the whistleblower has provided alternative contact details.

**§ 4. PROCEDURE FOR HANDLING AND REVIEWING INTERNAL REPORTS**

1. The responsibility for receiving and reviewing reports, taking follow-up actions, and maintaining contact with the whistleblower is entrusted to the Authorized Person.
2. Upon submission of the report, the whistleblower will receive confirmation of receipt within 7 (seven) days from the date of receipt.
3. After receiving and confirming the report, the Authorized Person conducts a preliminary analysis to assess whether the provided information constitutes a breach of law and whether the information allows for the initiation of an explanatory proceeding. At this stage, the Authorized Person may request additional information or clarification from the whistleblower.
4. The Authorized Person may refrain from reviewing the report and conducting the explanatory proceeding only if the report is clearly false or if, despite efforts, it has been impossible to obtain the necessary information from the whistleblower to review the report and conduct the explanatory proceeding.
5. If the report contains information about a breach of law and the available data is sufficient to consider the report credible and to conclude that there is a probability of a breach of law or irregularities within the Entity, the Authorized Person will initiate an explanatory proceeding.
6. The Authorized Person conducts the explanatory proceeding independently unless the nature of the report and the evidence presented require the involvement of other persons. The Authorized Person may seek the support of an independent and impartial expert if their knowledge and experience may be useful in conducting the explanatory proceeding. The expert may be appointed as an Authorized Person if they belong to the organizational structure of the Entity. In such a case, the Entity authorizes the expert to conduct the explanatory proceeding in writing and requires them to maintain the confidentiality of the personal data and information obtained, even after the conclusion of the proceeding. If the expert is not part of the Entity's structure, they are not considered an Authorized Person and cannot be granted access to personal data or any information that could reveal the identity of the whistleblower or individuals mentioned in the report. In this case, the expert serves only in an advisory role.
7. If the Authorized Person is the individual to whom the report pertains, they will be excluded from the process of reviewing the report. The Authorized Person may also voluntarily disclose circumstances that disqualify them or may affect their objectivity and impartiality. In such a case, the Entity will appoint another person to review the report.
8. The Authorized Person conducting the explanatory proceeding acts in accordance with the principles of fairness, impartiality, confidentiality, and the rules specified in this Procedure, and in cases not regulated by this Procedure – in accordance with the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws 2024, item 928).
9. The Authorized Person protects the whistleblower by taking measures to prevent the disclosure of their identity to third parties and any forms of retaliation, such as unequal treatment, mobbing, or harassment. This protection also extends to individuals close to the whistleblower, related to the whistleblower, or assisting them in submitting the report.
10. To clarify the circumstances mentioned in the report, the Authorized Person has the right to conduct confidential meetings with other employees or associates, particularly those mentioned in the report as witnesses to the breach of law. The Authorized Person prepares a written note from each meeting, and the explanations and information obtained from the individuals summoned are recorded in the protocol.

**§ 5. PROCEDURE FOR TAKING FOLLOW-UP ACTIONS**

1. After the explanatory actions are completed, the Authorized Person decides whether to take follow-up actions or refrain from them if the report is found to be groundless.
2. In the course of follow-up actions, the Authorized Person may recommend and take specific corrective or disciplinary actions against the person who committed the breach of law. These actions may include initiating additional explanatory proceedings, control, or administrative proceedings, as well as filing accusations, lawsuits, or other actions aimed at pursuing claims against the person who committed the breach of law.
3. The task of the Authorized Person also includes proposing preventive measures to eliminate similar breaches of law in the future.
4. Within 3 months from the date of confirming the report, the Authorized Person provides the whistleblower with feedback on the planned or taken follow-up actions and the reasons for those actions. If no confirmation was provided to the whistleblower, the 3-month period is counted from 7 days after the submission of the report unless the whistleblower did not provide a contact address for feedback.

**§ 6. REGISTER OF REPORTS**

1. The Authorized Person is required to maintain a register of all submitted reports.
2. The register of reports contains:
* the report number,
* the subject of the breach,
* the personal data of the whistleblower and the person to whom the report pertains, necessary for their identification,
* the contact address of the whistleblower,
* the date of the report,
* information on the actions taken in response,
* the date the case was closed.
1. The register is maintained in compliance with confidentiality principles, and all information concerning the report is stored in the register for 3 years after the end of the calendar year in which the follow-up actions were completed or after the proceedings initiated by these actions were concluded.

**§ 7. PROTECTION MEASURES FOR WHISTLEBLOWERS AND OTHER PERSONS**

1. It is prohibited to take any actions, threats, or attempts to hinder the whistleblower, a person associated with the whistleblower, or a person who assisted the whistleblower in submitting the report, to worsen their working conditions, discriminate against them, or engage in other types of unfair treatment in connection with the whistleblower's submission of a report in good faith.
2. In the case of work or services provided on the basis of other legal relations than employment, the provisions of § 7 section 1 apply accordingly, and the submission of a report or public disclosure cannot be the basis for retaliatory actions, attempts, or threats of such actions, including the termination of a contract, particularly concerning the sale or delivery of goods or the provision of services, withdrawal from such a contract without notice, or the imposition of obligations or the refusal to grant, limit, or revoke rights, especially licenses, permits, or exemptions.
3. The Authorized Person is responsible for ensuring the confidentiality of the submitted report and is obligated to respond appropriately to any indications of retaliatory actions or the disclosure of the whistleblower's identity.
4. Persons mentioned in § 7 section 1 above have the right to immediately notify the Authorized Person of retaliatory actions taken against them or the disclosure of their identity.
5. The whistleblower and the persons mentioned in § 7 section 1 above, who have been subjected to retaliatory actions, have the right to:
* compensation in an amount not less than the average monthly salary in the national economy in the previous year, announced for pension purposes in the Official Journal of the Republic of Poland "Monitor Polski" by the President of the Central Statistical Office, or
* redress for harm suffered.
1. A person who has suffered harm due to the whistleblower's deliberate submission of a false report or public disclosure of false information has the right to compensation or redress for the violation of personal rights from the whistleblower who made such a report or public disclosure.

**§ 8. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA**

1. The established reporting channels ensure the completeness, confidentiality, and integrity of the data, including its protection from unauthorized access. The Entity ensures that these channels allow for the permanent storage of information to facilitate further explanatory proceedings and prevent unauthorized persons from accessing the information contained in the report. The reporting channels guarantee the confidentiality of the whistleblower's identity and the identity of the person to whom the report pertains.
2. The whistleblower's personal data, which may reveal their identity, will not be disclosed to unauthorized persons unless the whistleblower gives explicit consent.
3. Personal data is processed only to the extent necessary to receive the report or to take follow-up action. Personal data that is irrelevant to the review of the report is not collected, and if it is accidentally collected, it is promptly deleted, no later than 14 days after it is determined that the data is irrelevant to the case.
4. Personal data is deleted after 3 years following the end of the calendar year in which the follow-up actions or the proceedings initiated by these actions are completed.

**§ 9. CRIMINAL LIABILITY**

1. Any person who prevents or significantly hinders another person from submitting a report is subject to a fine, restriction of liberty, or imprisonment for up to one year. If the person uses violence, an unlawful threat, or deception against another person, they are subject to imprisonment for up to 3 years.
2. Any person who takes retaliatory actions against a whistleblower, a person assisting in submitting the report, or a person associated with the whistleblower is subject to a fine, restriction of liberty, or imprisonment for up to 2 years. If the retaliatory actions are persistent, the person is subject to imprisonment for up to 3 years.
3. Any person who unlawfully discloses the identity of the whistleblower, the person assisting in submitting the report, or a person associated with the whistleblower is subject to a fine, restriction of liberty, or imprisonment for up to one year.
4. Any person who submits a report or makes a public disclosure knowing that no breach of law has occurred is subject to a fine, restriction of liberty, or imprisonment for up to 2 years.

**§ 10. FINAL PROVISIONS**

1. Provisions of collective labor agreements, internal regulations, and statutes, employment contracts, and other acts establishing employment relationships or governing the rights and obligations of the parties to the employment relationship, that directly or indirectly exclude or limit the right to submit an internal report, external report, or public disclosure, or that provide for retaliatory measures, are invalid.
2. The Entity makes this Procedure available for inspection in a place accessible to Employees and associates, and informs about the Procedure at the beginning of recruitment or negotiations preceding the conclusion of a contract with individuals seeking employment or other legal relations forming the basis for the provision of work or services.
3. This Procedure comes into effect 7 days after it is made available to the persons performing work in a manner accepted by the Entity.

**§ 6. REGISTER OF REPORTS**

The Authorized Person is required to maintain a register of all submitted reports.

The register of reports contains:

* the report number,
* the subject of the breach,
* the personal data of the whistleblower and the person to whom the report pertains, necessary for their identification,
* the contact address of the whistleblower,
* the date of the report,
* information on the actions taken in response,
* the date the case was closed.

The register is maintained in compliance with confidentiality principles, and all information concerning the report is stored in the register for 3 years after the end of the calendar year in which the follow-up actions were completed or after the proceedings initiated by these actions were concluded.

**§ 7. PROTECTION MEASURES FOR WHISTLEBLOWERS AND OTHER PERSONS**

It is prohibited to take any actions, threats, or attempts to hinder the whistleblower, a person associated with the whistleblower, or a person who assisted the whistleblower in submitting the report, to worsen their working conditions, discriminate against them, or engage in other types of unfair treatment in connection with the whistleblower's submission of a report in good faith.

In the case of work or services provided on the basis of other legal relations than employment, the provisions of § 7 section 1 apply accordingly, and the submission of a report or public disclosure cannot be the basis for retaliatory actions, attempts, or threats of such actions, including the termination of a contract, particularly concerning the sale or delivery of goods or the provision of services, withdrawal from such a contract without notice, or the imposition of obligations or the refusal to grant, limit, or revoke rights, especially licenses, permits, or exemptions.

The Authorized Person is responsible for ensuring the confidentiality of the submitted report and is obligated to respond appropriately to any indications of retaliatory actions or the disclosure of the whistleblower's identity.

Persons mentioned in § 7 section 1 above have the right to immediately notify the Authorized Person of retaliatory actions taken against them or the disclosure of their identity.

The whistleblower and the persons mentioned in § 7 section 1 above, who have been subjected to retaliatory actions, have the right to:

* compensation in an amount not less than the average monthly salary in the national economy in the previous year, announced for pension purposes in the Official Journal of the Republic of Poland "Monitor Polski" by the President of the Central Statistical Office, or
* redress for harm suffered.

A person who has suffered harm due to the whistleblower's deliberate submission of a false report or public disclosure of false information has the right to compensation or redress for the violation of personal rights from the whistleblower who made such a report or public disclosure.

**§ 8. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA**

The established reporting channels ensure the completeness, confidentiality, and integrity of the data, including its protection from unauthorized access. The Entity ensures that these channels allow for the permanent storage of information to facilitate further explanatory proceedings and prevent unauthorized persons from accessing the information contained in the report. The reporting channels guarantee the confidentiality of the whistleblower's identity and the identity of the person to whom the report pertains.

The whistleblower's personal data, which may reveal their identity, will not be disclosed to unauthorized persons unless the whistleblower gives explicit consent.

Personal data is processed only to the extent necessary to receive the report or to take follow-up action. Personal data that is irrelevant to the review of the report is not collected, and if it is accidentally collected, it is promptly deleted, no later than 14 days after it is determined that the data is irrelevant to the case.

Personal data is deleted after 3 years following the end of the calendar year in which the follow-up actions or the proceedings initiated by these actions are completed.

**§ 9. CRIMINAL LIABILITY**

1. Any person who prevents or significantly hinders another person from submitting a report is subject to a fine, restriction of liberty, or imprisonment for up to one year. If the person uses violence, an unlawful threat, or deception against another person, they are subject to imprisonment for up to 3 years.
2. Any person who takes retaliatory actions against a whistleblower, a person assisting in submitting the report, or a person associated with the whistleblower is subject to a fine, restriction of liberty, or imprisonment for up to 2 years. If the retaliatory actions are persistent, the person is subject to imprisonment for up to 3 years.
3. Any person who unlawfully discloses the identity of the whistleblower, the person assisting in submitting the report, or a person associated with the whistleblower is subject to a fine, restriction of liberty, or imprisonment for up to one year.
4. Any person who submits a report or makes a public disclosure knowing that no breach of law has occurred is subject to a fine, restriction of liberty, or imprisonment for up to 2 years.

**§ 10. FINAL PROVISIONS**

1. Provisions of collective labor agreements, internal regulations, and statutes, employment contracts, and other acts establishing employment relationships or governing the rights and obligations of the parties to the employment relationship, that directly or indirectly exclude or limit the right to submit an internal report, external report, or public disclosure, or that provide for retaliatory measures, are invalid.
2. The Entity makes this Procedure available for inspection in a place accessible to Employees and associates, and informs about the Procedure at the beginning of recruitment or negotiations preceding the conclusion of a contract with individuals seeking employment or other legal relations forming the basis for the provision of work or services.
3. This Procedure comes into effect 7 days after it is made available to the persons performing work in a manner accepted by the Entity.

**INFORMATION CLAUSE ON PERSONAL DATA PROCESSING**

* 1. Pursuant to Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, we inform you that:
	2. **DATA CONTROLLER**

The controller of your personal data is Finejas Poland Sp. z o.o., branch in Białystok, ul. Warszawska 6/32, 15-063 Białystok, NIP 9662138529, REGON: 381368762-00010 (hereinafter referred to as the Controller).

To obtain information regarding the processing and protection of personal data, you may contact the Controller in the following ways:

* by mail at: Kazimierza Michalczyka 5, 53-633 Wrocław
* by email: justyna.ginter@finejas.pl
* by phone: +48 572 097 854

**PURPOSE AND BASIS FOR DATA PROCESSING**

1. The data provided will be processed to fulfill the obligations specified in the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws 2024, item 928 – hereinafter referred to as the Act), in particular, to receive reports of legal violations and to take follow-up actions.
2. The basis for the processing of personal data is: a) a legal obligation arising from the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws 2024, item 928) – Article 6(1)(c) of the GDPR, b) consent in the case of the disclosure of the whistleblower’s identity – Article 6(1)(a) of the GDPR, c) the legitimate interest of the Controller or a third party whose data is disclosed, such as the necessity to verify the received report and conduct an explanatory investigation – Article 6(1)(f) of the GDPR.

**RIGHTS RELATED TO THE PROCESSING OF PERSONAL DATA**

1. You are entitled to the following rights related to the processing of personal data: a) the right to access the content of your data, b) the right to rectify or supplement your data, c) the right to withdraw consent to the disclosure of your identity, d) the right to erase your data, e) the right to object, and during the consideration of the report, the right to restrict the processing of your data, f) the right to file a complaint with the President of the Personal Data Protection Office (UODO).

**PRINCIPLES OF PERSONAL DATA PROCESSING**

1. The provision of personal data is voluntary, and the report may be submitted anonymously.
2. Personal data will not be disclosed to external entities, except to those authorized to receive internal reports and take follow-up actions, including verification of the report and further communication, as well as to the platform provider for report handling and other entities processing data under a data processing agreement with the Controller. Personal data may also be shared with entities authorized to receive it under other legal provisions, particularly public authorities.
3. Personal data and other information disclosed in the register of internal reports will be stored for 3 years after the end of the calendar year in which follow-up actions were completed or proceedings initiated by those actions were concluded.
4. Personal data processed in connection with the submission of a report or the taking of follow-up actions, as well as documents related to the report, will be stored for 3 years after the end of the calendar year in which the external report was submitted to the public authority competent to take follow-up actions or follow-up actions were completed, or after the conclusion of proceedings initiated by those actions.

**PROFILING AND TRANSFER OF PERSONAL DATA**

1. Personal data collected for the purpose of fulfilling a statutory obligation will not be subject to automated decision-making, including profiling.
2. The Controller will not transfer your personal data to recipients outside the EEA (third country or international organization).