Procedure for internal reporting of breaches of law

The procedure stemming from the Act on the Protection of Whistleblowers

Classification:	**Public** information
Version:	1.1
Last modification date:	11.09.2025

1. Scope of the Procedure

This document describes the internal procedure for reporting breaches of law and for follow-up actions at Future Processing S.A. (hereinafter referred to as the “**Company**”).

2. Definitions

Terms used herein have the following meaning:

1. **Follow-up**: any action taken by the Company to assess the accuracy of the information presented in the report and to address the breach reported, including, in particular, an investigation, the initiation of an inspection or administrative proceedings, prosecution, an action for recovery of funds or the closure of the procedure conducted as part of the internal procedure for reporting breaches of law and for follow-up actions or the procedure for receiving external reports and taking follow-up actions.

2. **Retaliation**: any direct or indirect act or omission in the work-related context which is prompted by reporting or by public disclosure, and which violates or may violate the rights of or causes or may cause unjustified detriment to the whistleblower, including the illegitimate initiation of proceedings against the whistleblower.

3. **Information on breaches**: the information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the Company in which the whistleblower took part in recruitment or other negotiations preceding the execution of the agreement, works or worked, or in with which the whistleblower is or was in contact in the work-related context, or information about attempts to conceal such breaches.

4. **Feedback**: the provision to the whistleblower of information on the action envisaged or taken as follow-up and on the grounds for such follow-up.

5. **Internal unit**: an impartial internal business unit or person within the organisational structure of the Company which or who is authorised to receive the reports and take follow-up actions, including the verification of internal reports and further communication with the whistleblower, including an enquiry for additional information and the provision of feedback to the whistleblower.

6. **Work-related context**: current or future work-related activities based on employment or on another legal relationship on the basis of which work is provided or based on services or a function performed in or for the Company or serving in the Company through which persons acquire information on breaches and within which those persons could suffer retaliation.

7. **Public authority:** the highest and central government administration authorities, local government administration authorities, authorities of local government units, other state authorities and other entities that perform public administration duties by law, which are competent to take follow-up actions in the fields stipulated in Art. 3.1 of the Act on the Protection of Whistleblowers.

8. **Person concerned:** a natural person, a legal person or an unincorporated business entity with legal capacity, as set out in the Act, who or which is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated.

9. **Facilitator**: a natural person who assists a whistleblower in the reporting process or public disclosure in the work-related context, and whose assistance should be confidential.

10. **Person connected with the whistleblower:** a natural person who may experience retaliation, including the whistleblower's colleague or closest person within the meaning of Art. 115 § 11 of the Criminal Code of 6 June 1997 (Journal of Laws No 2024.17).

11. **Legal entity**: a private or public entity.

12. **Private entity:** a natural person carrying out business activity, a legal person or an unincorporated business unit which has legal capacity by law or an employer, provided that they are not public entities; in this case: the Company.

13. **Public entity**: an entity specified in Art. 3 of the Act of 11 August 2021 on open data and re-use of information of the public sector (Journal of Laws No 2023.1524).

14. **Legal proceedings**: proceedings conducted on the basis of commonly applicable legal regulations, including in particular criminal, civil, administration, disciplinary proceedings or proceedings concerning the violation of public finance discipline, or proceedings conducted on the basis of internal regulations issued to implement commonly applicable legal (in particular anti-mobbing) regulations.

15. **Whistleblower**: a natural person who reports or publicly discloses information about breaches of law acquired in the work-related context of the Company.

16. **Public disclosure**: the making of information on breaches available in the public domain.

17. **Report**: an oral or written internal or external report made in accordance with the requirements of the Act.

18. **Internal reporting**: verbal or written communication of information on breaches within the legal entity.

19. **External reporting**: verbal or written communication of information on breaches to the Ombudsman or a public authority.

3. Receiving reports

3.1. Breach of law

Reports may include acts or omissions that are unlawful or aim at circumventing law and are related to:

1) corruption;
2) public procurement;
3) financial services, products and markets;
4) counteracting money laundry and terrorism financing;
5) product safety and compliance;
6) transport safety;
7) environmental protection;
8) radiological protection and nuclear safety;
9) food and feed safety;
10) animal health and welfare;
11) public health;
12) consumer protection;
13) privacy and personal data protection;
14) ICT network and system security;
15) financial interests of the State Treasury of the Republic of Poland, local government units and the European Union;
16) the internal market of the European Union, including public legal principles applicable to competition and state aid, as well as the taxation of legal persons;
17) constitutional freedoms and rights of human beings and citizens, as applicable in the organisation's relationships with public authorities and not related to the fields referred to in sections 1-16.

3.2. Reporting channel

1. Reports should be made by e-mail at the following e-mail address whistleblowers@future-processing.com.

2. If the report is made otherwise, the whistleblower will be requested to send the report to the dedicated e-mail address to enable the verification of the report and the follow-up.

3. In the case of reports made otherwise than through the above channel, the Company does not guarantee that the whistleblower will be protected in accordance with this procedure.

4. The report must include all necessary information which will let the Company effectively initiate the verification of the report and the follow-up, including, for example:

    a. Date and time of the breach;

    b. Description of the breach;

    c. Information about a person/persons causing the breach (forename, surname, other identification information);

    d. Information about other persons that, in the reporting person's opinion, may have further information about the breach;

    e. Any other information that, in the reporting person's opinion, may be helpful.

3.3. Anonymous report and identity verification

1. The Company does not accept anonymous reports (i.e. reports sent from an unknown e-mail address or reports without identification data or data allowing for the verification of the sender's identity).
2. Having received an anonymous report, the Company will try to obtain the whistleblower's identification data by contacting the whistleblower.
    a. If the whistleblower discloses his or her identity, the report will be handled on a normal basis.
    b. In the event the whistleblower cannot be identified, the report will not be taken into consideration.
3. If the identity of the whistleblower is doubtful, the Company may request further information in order to confirm the identity of that person.
4. In the event the report is submitted via a known e-mail address (in particular a business e-mail address assigned to a specific natural person), the internal unit may confirm whether the report is authentic by contacting the whistleblower in person.

4. Handling the report

4.1. Internal unit handling the report

1. In the Company there is an internal unit that is responsible for receiving internal reports and taking follow-up actions.
2. Members of the internal unit are authorised in writing by the Company to handle the report, including access to the whistleblower's personal data.
3. Members of the internal unit make sure that the report is handled in an impartial way.
4. Having any doubts about his or her impartiality due to the character of the report, the member of the internal unit will immediately stop handling the report and the report will be handled by other members of the unit.
5. The information about the existing members of the internal unit is provided on request and published in the Company's internal network (intranet).

4.2. Confirmation that the report has been accepted

1. The internal unit will confirm that the report has been accepted within 7 days of the receipt.
2. The confirmation will be sent to the e-mail address from which the report is sent, unless the whistleblower specifies another contact address in the report (then the confirmation will be sent to such an e-mail address).

4.3. Follow-up

1. The internal unit assesses all circumstances of the reported breach of law in accordance with the impartiality rule.
2. If necessary, the internal unit takes actions to obtain further explanations and may, in particular, contact persons having any knowledge concerning the report (including the whistleblower and person concerned).
3. The internal unit makes sure that the whistleblower remains anonymous (even before the Board of Directors of the Company) during all actions.
4. The internal unit respects personal rights and protects the reputation of other persons taking part in the clarification of the circumstances of the report.
5. Upon the investigation, the internal unit assesses the evidence in a comprehensive way and presents a statement on the investigation, the assessment of the legitimacy of the report and recommendations, if any, concerning necessary actions, to the Directors.
6. The final decision to take necessary follow-up actions is made by the Directors based on the statement prepared by the internal unit.
7. The report together with the statement are entered in the internal record of reports.

4.4. Deadline for feedback

1. Within 3 months of the confirmation of the acceptance of the report or, if the confirmation is not submitted to the reporting person, within 3 months from the expiry of 7 days of the report, the internal unit notifies the whistleblower of follow-up actions taken by the Company.

5. Record keeping of the reports

1. The Company keeps the internal record of the reports of breaches of law.
2. The record is kept by the internal unit.
3. The record is only accessible to members of the internal unit.
4. The record includes the following data:
    a. The number of the report;
    b. The object of breach of law;
    c. Personal data of the whistleblower and the person concerned, as necessary to identify those persons;
    d. The whistleblower's contact address;
    e. The reporting date;
    f. Information on follow-up;
    g. The closure date.
5. The statement on the investigation is also recorded together with the report.
6. If reasonable (e.g. to analyse the report), the data kept in the record may be made available to other persons (without prejudice to the whistleblower's anonymity).

6. Protection of the whistleblower’s data

6.1. Disclosure of the whistleblower’s data

1. The whistleblower’s personal data based on which the whistleblower can be identified will be only known to members of the internal unit and will not be disclosed to unauthorised persons, unless with the whistleblower’s explicit consent.
2. The whistleblower’s personal data may be disclosed (if permitted by law) to other entities in connection with the investigation conducted by public authorities or preparatory or court proceedings conducted by courts, for example to protect the right to defence attributable to the person concerned, however solely if such disclosure is necessary and proportionate.

6.2. Duration of the processing

1. The personal data and other information kept in the record of internal reports will be retained for 3 years of the end of the calendar year in which follow-up actions are terminated or of the end of proceedings initiated by such actions.
2. Personal data that insignificant for the investigation will not be collected and, if collected accidentally, will be erased immediately (within no more than 14 days of the moment they are found to be insignificant for the investigation).

7. External reporting

7.1. Reporting breaches to the Ombudsman

1. The person may report breaches of law externally directly to the Ombudsman without prior internal report.
2. The reports may be delivered to the Ombudsman:

    a. via the Internet by use of an online form available at: https://sygnalisci.brpo.gov.pl/

    b. in writing to the following address:
    Biuro Rzecznika Praw Obywatelskich (Ombudsman's Office)
    al. Solidarności 77
    00-090 Warszawa (Warsaw)

    c. in person at the Ombudsman's offices in Warsaw, Katowice, Gdańsk or Wrocław or during the Ombudsman's office hours in other cities of Poland. Detailed information about the addresses and office hours is published on the Ombudsman's website: https://bip.brpo.gov.pl/pl/content/punkty-przyjec-interesantow

    d. verbally – via a recorded telephone hotline at the number indicated on the Ombudsman's website at: www.sygnalisci.gov.pl and in accordance with the indicated working hours.

3. Valid and detailed information on reporting to the Ombudsman is available on the Ombudsman's website:
https://bip.brpo.gov.pl/pl/content/zlozenie-wniosku-do-rzecznika-praw-obywatelskich

7.2. Reporting breaches to other public authorities

1. The person may report breaches externally directly to a relevant public authority and, if applicable, to institutions, authorities or business units of the European Union.

2. The report must be made on the basis of relevant regulations and in accordance with procedures applicable to the relevant institution.

8. Miscellaneous

1. This Procedure comes into force as of 07.10.2024 upon prior consultation with representatives of persons working for Future Processing S.A.
2. This Procedure may be amended at any time for relevant reasons (e.g. necessary updates). The amended procedure will come into force 7 days of its publication date.
3. The binding version of this Procedure will be made available on request.