Directive

Aptitude Software (Poland) sp. z o.o. with its registered office in Wrocław (the Company)

issued on 24.10.2024.

Regarding the Implementation of the Procedure for Reporting Legal Violations and Taking Follow-up Actions

Based on Article 24 of the Act of June 14, 2024, on the Protection of Whistleblowers (Journal of Laws 2024, item 928) (hereinafter referred to as the "Act"), the Company resolves:

§ 1

To establish the Procedure for Reporting Legal Violations and Taking Follow-up Actions as set forth in the attachment to this Directive.

§ 2

This Directive shall enter into force 7 days after being communicated to the employees of the Company through the means adopted by the Company, namely via the intranet network in the Connect HR or SharePoint system.

PROCEDURE

FOR REPORTING LEGAL VIOLATIONS AND TAKING FOLLOW-UP ACTIONS

at Aptitude Software (Poland) sp. z o.o. with registered office in Wroclaw

dated 24.10.2024.

§1

GENERAL PROVISIONS

1. This Procedure sets out the rules and conditions for establishing an internal channel and procedures for the purpose of making internal reports and taking follow-up actions at Aptitude Software (Poland) sp. z o.o. based in Wrocław.
2. The acceptance of reports of legal violations, procedures, and standards is an element of proper and safe management at Aptitude Software (Poland) Ltd. and serves to increase the efficiency of detecting irregularities and taking actions to eliminate them and reduce risk at all organizational levels.
3. The implemented reporting system enables the reporting of irregularities through special, easily accessible channels, in a manner that ensures reliable and independent recognition of the report and provides protection against retaliatory, repressive, discriminatory, or other types of unfair treatment in connection with the report made.

4. Terms Used in the Procedure Mean:

a) Personal Data - information relating to an identified or identifiable natural person;

b) Follow-up Actions - actions taken [by the Company] to assess the truthfulness of the information contained in the report and, where appropriate, to prevent the legal violation that is the subject of the report, including internal investigation, explanatory proceedings, initiation of control, filing of charges, actions taken to recover financial resources, or closure of the reporting and verification procedure;

c) Retaliatory Actions - direct or indirect actions or omissions in a work-related context that are caused by the report and that violate or may violate the rights of the Whistleblower or cause or may cause unjustified harm to the Whistleblower;

d) Feedback - providing the Whistleblower with information on planned or taken follow-up actions and the reasons for these follow-up actions;

e) Whistleblower - a natural person who reports violations under this Procedure or the Act;

f) Person Concerned by the Report - a natural person, legal person, or organizational unit without legal personality, to whom the Act grants legal capacity, indicated in the report as the person who committed the legal violation or as a person associated with the person who committed the legal violation;

g) Person Assisting in Making the Report - a natural person who assists the Whistleblower in making the report or public disclosure in a work-related context and whose assistance should not be disclosed;

h) Person Associated with the Whistleblower - a natural person who may experience retaliatory actions, including a co-worker or a close person to the Whistleblower;

i) Authorized Person - a person designated by the data controller to perform the duties specified by the data controller in the field of personal data processing;

j) Procedure - the Procedure for Reporting Legal Violations and Taking Follow-up Actions at Aptitude Software (Poland) sp z o.o. based in Wrocław;

k) Company - Aptitude Software (Poland) Ltd.;

l) Act - the Act of June 14, 2024, on the Protection of Whistleblowers (Journal of Laws 2024, item 928);

m) Internal Report (hereinafter referred to in this Procedure as Internal Report or Report) - as referred to in this Procedure, the written submission of information about a legal violation, in the manner specified in the further part of the Procedure;

n) External Report - means the oral or written submission of information about a legal violation to the Ombudsman or a public authority.

§2
SUBJECT OF THE REPORT, ACCEPTANCE OF REPORTS

1. The purpose of the procedure is to effectively detect cases of legal violations mentioned in paragraph 2 below, prevent illegal activities, and improve working conditions in the Company.
2. The subject of the Report may include any actions or omissions that are illegal or aim to circumvent the law concerning:

   a) Corruption;

   b) Public procurement;

   c) Services, products, and financial markets;

   d) Anti-money laundering and counter-terrorism financing;

   e) Product safety and compliance with requirements;

   f) Transport safety;

   g) Environmental protection;

   h) Radiological protection and nuclear safety;

   i) Food and feed safety;

   j) Animal health and welfare;

k) Public health;

l) Consumer protection;

m) Privacy and personal data protection;

n) Network and information systems security;

o) Financial interests of the State Treasury of the Republic of Poland, local government units, and the European Union;

p) The internal market of the European Union, including public competition and state aid rules, and corporate taxation;

q) Constitutional freedoms and human and civil rights – occurring in relations between individuals and public authorities and not related to the areas specified in points a)-p).

3. It is recommended to make reports through the internal channel.
4. The People & Culture department is responsible for ensuring the implementation of the Procedure.
5. The following are responsible for performing tasks arising from the Procedure:

   a) [People Partner, People Director, HR Administration Specialist, SVP of People & Culture] – maintaining the report register;

   b) [People Partner, People Director, HR Administration Specialist, SVP of People & Culture] – receiving and verifying Reports (including confirming receipt of Reports);

   c) [People Partner, People Director, HR Administration Specialist, SVP of People & Culture] – taking follow-up actions, providing feedback;

   d) [People Partner, People Director, HR Administration Specialist, SVP of People & Culture] – coordinating within the Company the tasks mentioned in points a) - c).
6. The Company may use external advisors, including lawyers, legal advisors, tax advisors, or other persons whose specialized knowledge will be necessary for the proper performance of the aforementioned activities, in matters of verifying Reports or making decisions on follow-up actions.
7. Only persons with written authorization from the Company, including authorization to process Personal Data and a confidentiality statement, may be allowed to receive and verify Reports, take follow-up actions, and process personal data of individuals.
8. The authorization and confidentiality statement referred to in § 2 paragraph 7 of the Procedure are attached as Annexes 1 and 2 to this Procedure.

§3
PERSONS AUTHORIZED TO MAKE A REPORT, REPORTING CHANNELS

1. Irregularities may be reported by an employee and:

a) a temporary worker;

b) a person performing work on a basis other than an employment relationship, including under a civil law contract;

c) an entrepreneur;

d) a proxy;

e) a shareholder or partner;

f) a member of the body of a legal person or an organizational unit without legal personality;

g) a person performing work under the supervision and direction of a contractor, subcontractor, or supplier, including under a civil law contract;

h) an intern;

i) a volunteer;

j) a trainee; and

k) other persons indicated in Article 4(1) and (2) of the Act.

2. An internal report should be submitted via: a) email address: whistle-blower-poland@aptitudesoftware.com ;
3. The report in the system specified in paragraph 2(a) should be formulated in Polish or in English (in the case of foreigners).
4. The administrator of the system specified in paragraph 2(a) will be the Company.
5. Anonymous reports will not be considered.

§4
MAKING REPORTS

1. The report should include, in particular:

   a) the Whistleblower's name and surname;

   b) contact address – email address or correspondence address;

   c) date and place of the report;

   d) description of the irregularity along with the identification of the person who committed the violation.

2. It is also recommended that the report includes a clear and complete explanation of the subject of the report and at least the following information: the date and place of the legal violation or the date and place of obtaining information about the legal violation, a description of the specific situation or circumstances creating the possibility of a legal violation, identification of any witnesses to the legal violation, and identification of known evidence and information that may be helpful in the process of considering the report.

3. The Whistleblower should have reasonable grounds to believe that the information about the violation being reported is true at the time of making the report and that such information constitutes information about a legal violation.
4. Making a report of false information, despite the lack of grounds to believe that the information about the violation being reported is true at the time of making the report, may be grounds for taking disciplinary action against the Whistleblower and is also subject to criminal liability if the Whistleblower knew that such a legal violation did not occur.

§5
ANALYSIS OF REPORTS, EXPLANATORY PROCEEDINGS

Confirmation of receipt of the Report will occur within 7 days of receiving the Report, unless the Whistleblower has not provided a contact address to which the confirmation should be sent or the provided address is incorrect.

1. The unit responsible for receiving and considering the Report verifies it while maintaining confidentiality, impartiality, and objectivity.
2. The internal channel provided by the Company ensures the security and confidentiality protection of the Whistleblower and third parties mentioned in the Report.
3. The confidentiality mentioned in paragraphs 2 and 3 will be ensured by:

   a) restricting access to information - only for Authorized Persons;

   b) obtaining written statements from Authorized Persons regarding their obligation to maintain the confidentiality of information obtained during the procedure;

   c) making Reports in the system located at the internet address: whistle-blower-poland@aptitudesoftware.com, which meets all IT security and personal data protection requirements, including compliance with information security management system requirements;

   d) applying appropriate legal provisions to persons who disclose confidential information.
4. The person specified in § 2 paragraph 5 letter c of the Procedure takes follow-up actions without undue delay and with due diligence.
5. Follow-up actions primarily include:

   a) conducting an internal investigation, which involves, among other things, collecting evidence related to the violation, examining the facts, requesting additional information, etc.;

   b) conducting explanatory proceedings aimed at confirming or refuting the facts contained in the Report, including through consultations; taking actions against the person who violates the law depending on the violation committed - conducting a conversation, terminating the contract, filing a complaint with the appropriate authority, initiating appropriate proceedings, etc.;

c) taking all possible actions to prevent incidents covered by the Report in the future, including ongoing monitoring of Reports, auditing, conducting training, courses.

6. As a result of the follow-up actions taken, the Report may be:

   a) accepted – the Report is justified, follow-up actions will be taken without undue delay or the appropriate authorities will be notified;

   b) dismissed – the Report is unfounded or does not fall under this Procedure, or the violation described in the Report is untrue.

7. The person specified in § 2 paragraph 5 letter c of the Procedure provides feedback to the Whistleblower within a maximum of 3 months from the confirmation of receipt of the Report or – in the case of not providing the confirmation mentioned in paragraph 1 – 3 months from the expiration of 7 days from the date of making the Report, unless the Whistleblower has not provided a contact address to which the feedback should be sent.

§6
REGISTER OF REPORTS

1. The Company maintains a register of internal reports made through the internal channel, exercising due diligence.
2. Data entry into the register of reports is based on the internal report.
3. The following data is collected in the register of internal reports:

   a) report number;

   b) subject of the legal violation;

   c) personal data of the Whistleblower and the person concerned by the report, necessary for identifying these persons;

   d) contact address of the Whistleblower;

   e) date of the report;

   f) information on follow-up actions taken;

   g) date of case closure.

4. The Company implements technical and organizational solutions to ensure the storage of the Whistleblower's personal data separately from the document or other information carrier containing the report, including, where appropriate, the immediate removal of all personal data of the Whistleblower from the content of the document or other information carrier upon receipt.
5. Personal data and other information in the register of reports are stored for a period of 3 years after the end of the calendar year in which the follow-up actions were completed or after the conclusion of proceedings initiated by these actions.

§7
PROHIBITION OF RETALIATORY ACTIONS

1. The Company ensures protection against retaliatory actions for the Whistleblower and the person assisting in making the report, provided that the Whistleblower or the assisting person has an employment relationship with the Company or performs work or provides services for the Company on a basis other than an employment relationship. This provision also applies to persons associated with the Whistleblower.
2. Retaliatory actions are considered to include, in particular:
   a) refusal to establish an employment relationship;
   b) termination or dismissal without notice of the employment relationship;
   c) failure to conclude a fixed-term or indefinite-term employment contract after the termination of a probationary employment contract, failure to conclude another fixed-term employment contract or an indefinite-term employment contract after the termination of a fixed-term employment contract – in situations where the Whistleblower had a reasonable expectation that such a contract would be concluded;
   d) reduction in the amount of remuneration for work;
   e) withholding promotion or omission in promotion;
   f) omission in granting work-related benefits other than remuneration or reduction in the amount of such benefits;
   g) transfer of the employee to a lower position;
   h) suspension from performing work duties;
   i) assignment of the employee's current duties to another employee;
   j) unfavorable change in the place of work or work schedule;
   k) negative performance evaluation or negative work opinion;
   l) imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature;
   m) coercion, intimidation, or exclusion;
   n) mobbing;
   o) discrimination;
   p) unfavorable or unfair treatment;
   q) withholding participation or omission in nominating for participation in professional qualification training;
   r) unjustified referral for medical examination, including psychiatric examination, unless separate regulations provide for the possibility of referring an employee for such an examination;
   s) actions aimed at hindering future employment in a given sector or industry based on an informal or formal sectoral or industry agreement;
   t) causing financial loss, including economic loss or loss of income;
   u) causing other material damage, including violation of personal rights, in particular the good name of the Whistleblower.
3. Retaliatory actions are also considered to include threats or attempts to apply the measures listed in paragraph 2.

4. In cases where work or services were or are to be performed on a basis other than an employment relationship, retaliatory actions are understood to be actions similar to those listed in paragraph 2 above, if the nature of the work or function performed does not exclude this (paragraphs 2 and 3 apply accordingly).
5. Protection against retaliatory actions is considered to include, in particular:
   a) actions guaranteeing the confidentiality of data at every stage of verification, as well as after its completion;
   b) taking actions, including disciplinary actions, not excluding termination of the contract without notice against the person who committed the violations and taking possible consequences against the person who took retaliatory actions against the Whistleblower;
   c) compliance by the Company with the principles of equal treatment and non-discrimination indicated in the Labor Code.
6. In the event that the Company engages in retaliatory actions against the Whistleblower, the Whistleblower has the right to compensation in an amount not less than the average monthly remuneration 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 the right to redress.
7. Preventing and hindering reports and disclosing the identity of the Whistleblower, the person assisting in making the report, or the person associated with the Whistleblower contrary to the provisions of the Act, is subject to a fine, restriction of liberty, or imprisonment for up to one year.
8. Taking retaliatory actions against the Whistleblower, the person assisting in making the report, or the person associated with the Whistleblower is subject to a fine, restriction of liberty, or imprisonment for up to two years.

§8
PERSONAL DATA PROTECTION

1. The Company is the data controller of the data collected in the register specified in §6 of this Procedure.
2. The personal data of the Whistleblower, the Person Concerned by the Report, and other persons are processed by the Company as the Data Controller in a manner that ensures compliance with the relevant personal data protection regulations.
3. The confidentiality of the Whistleblower's identity will be treated in accordance with legal provisions, and therefore, in exceptional cases, the identity may be disclosed to the person(s) concerned by the report.
4. Personal data processed in connection with the receipt of the Report is stored by the Company for the periods specified by law.
5. The content of the information on the processing of personal data necessary to be provided in connection with the report of irregularities will be determined by a separate directive of the Company.

§9
EXTERNAL REPORTS

1. An external report may be made at any time to the Ombudsman or a public authority, bypassing the reporting procedure provided for in this Procedure (External Report), particularly when:

   a) within the timeframe for providing feedback, the Company does not take follow-up actions or does not provide feedback to the Whistleblower;

   b) the Whistleblower has reasonable grounds to believe that the legal violation may pose a direct or obvious threat to the public interest, especially if there is a risk of irreversible harm;

   c) making an internal report would expose the Whistleblower to retaliatory actions;

   d) in the case of making an internal report, there is little likelihood of effectively preventing the legal violation by the Company due to the specific circumstances of the case, such as the possibility of hiding or destroying evidence or the possibility of collusion between the Company and the perpetrator of the legal violation or the Company's involvement in the legal violation.

2. An external report made to the Ombudsman or a public authority, bypassing the internal report, does not deprive the Whistleblower of the protection guaranteed by the Whistleblower Protection Act.

3. In appropriate cases, the Whistleblower may report to institutions, bodies, or organizational units of the European Union.

§10
FINAL PROVISIONS

1. Persons performing work, including employees, are required to familiarize themselves with the Procedure.
2. The content of the Procedure has been consulted with representatives of persons performing work for the Company.
3. This Procedure enters into force 7 days after its announcement in the manner adopted by the Company.
4. Changes to the Procedure can only be made in writing.
5. In matters not regulated by this Procedure, the relevant provisions of 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, the Whistleblower Protection Act, the Labor Code, the Code of Criminal Procedure, and the Penal Code apply.

……

Company

……

Representatives of persons performing work for the Company

Annex No. 1 to the Procedure dated 24.10.2024 regarding the reporting of legal violations and taking follow-up actions at Aptitude Software (Poland) Ltd. based in Wrocław

…….
(Company header stamp)

Wrocław, dated _____

AUTHORIZATION TO RECEIVE AND VERIFY REPORTS/TAKE FOLLOW-UP ACTIONS AND TO PROCESS PERSONAL DATA*

Acting on behalf of Aptitude Software (Poland) Ltd. based in Wrocław, based on the provisions of the Procedure for reporting legal violations and taking follow-up actions (hereinafter referred to as the "Procedure"), hereby:

§ 1

Authorization to receive and verify reports/take follow-up actions*

1. I authorize Mr./Ms. _____ to receive and verify reports/take follow-up actions*.
2. The authorization is issued for the duration of the specified functions and may be revoked by the Company at any time.

§ 2

Authorization to process personal data

1. I authorize Mr./Ms. _____ to process the following categories of personal data concerning employees of Aptitude Software (Poland) Ltd. based in Wrocław, temporary workers, persons performing work for Aptitude Software (Poland) Ltd. based in Wrocław on a basis other than an employment relationship, including under a civil law contract, entrepreneurs, proxies, shareholders and partners, members of the body of a legal person or an organizational unit without legal personality, persons performing work under the supervision and direction of a contractor, subcontractor or supplier, including under a civil law contract, interns, volunteers, trainees, and other persons indicated in Article 4(1) and (2) of the Whistleblower Protection Act: name, surname, address, contact details, personal data of the person concerned by the report, date of the report, information on follow-up actions taken, date of case closure, report number, subject of the legal violation to the extent necessary to perform tasks arising from the Procedure.

The authorization concerns the processing of data, among others, in the IT system at the address whistle-blower-poland@aptitudesoftware.com , in terms of access to this data, its collection, modification, and analysis.

2. The person authorized to process personal data within the scope mentioned in paragraph 1 is obliged to keep it confidential and to keep the means securing it confidential, even after the period of performing the functions has ended, as well as to comply with the regulations on personal data protection and internal regulations, rules, and instructions on personal data protection in force at Aptitude Software (Poland) Ltd. based in Wrocław.

3. The authorization is issued for the duration of the specified functions and may be revoked by the Company at any time.

_____

Signature of the person authorized to act on behalf of the Company

Annex No. 2 to the Procedure dated 24.10.2024 regarding the reporting of legal violations and taking follow-up actions at Aptitude Software (Poland) Ltd. based in Wrocław

Wrocław, dated _____

CONFIDENTIALITY STATEMENT

I, the undersigned _____, declare that in connection with the authorization granted to me on _____ to process personal data within the scope specified in the content of the said authorization (hereinafter referred to as the "Authorization"), I undertake to:

- keep confidential the personal data (and the means securing them) to which I will have access in connection with the performance of the tasks assigned to me under the Authorization, both during the validity of this Authorization and after its expiration/revocation;
- comply with the procedures in force at Aptitude Software (Poland) Ltd. based in Wrocław regarding the protection of personal data;
- not use the personal data to which I will have access in the course of the activities performed in accordance with the Authorization without the authorization of Aptitude Software (Poland) Ltd. based in Wrocław;
- not disclose information that constitutes a business secret, as well as the trade secret of the Company within the meaning of Article 11(2) of the Act on Combating Unfair Competition.

I declare that I have been acquainted with the regulations concerning the protection of personal data, in particular the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as well as national regulations concerning the protection of personal data.

_____

Signature