INTERNAL REPORTING RULES
OF CONTROLANT POLAND SP. Z O.O.
DATED AUGUST 1, 2025

1. 1. PURPOSES OF THE RULES

1.1. These Rules have been adopted by Controlant Poland Sp. z o.o. pursuant to Art. 24(1) of the Whistleblower Protection Act of 24 June 2024 (Journal of Laws of 2024 item 928).

1.2. The purpose of these Rules is to create and provide a secure and confidential channel of communication for employees and collaborators to report breaches of the law or irregularities that may occur at the Company. Furthermore, these Rules are introduced in order to:

1.2.1. protect the interests of the Company and its employees;

1.2.2. ensure the compliance of the Company's actions with the applicable laws;

1.2.3. promote ethical standards in the workplace;

1.2.4. prevent breaches of the law through early detection and appropriate Follow-up Actions;

1.2.5. protect Whistleblowers against Retaliation.

2. DEFINITIONS:

2.1. Act – the Whistleblower Protection Act of 24 June 2024 (Journal of Laws of 2024 item 928);

2.2. Breach – the Breach referred to in clause 3.1 of the Rules;

2.3. Company – Controlant Poland Spółka z ograniczoną odpowiedzialnością with its registered office in Wroclaw (50-082), at 1 ks. Piotra Skargi Street, entered in the register of entrepreneurs maintained by the District Court for Wrocław-Fabryczna in Wrocław, 6th Commercial Division of the National Court Register, under KRS No.: 0000927230, with NIP (tax identification number): 5272974256 and REGON (statistical number): 520205640;

2.4. Controlant Group – a group of companies to which the Company belongs, in particular all companies dominant in relations to the Company (parent company) as well as their subsidiaries, including the Company;

2.5. Confidential Information – information relating to or coming from a Whistleblower and connected with a Report (including the Whistleblower's identity) that is confidential in nature and is treated by the Company on a confidential basis;

2.6. External Report – the communication of information to a public authority or the Ombudsman or entities, bodies or institutions of the European Union on an act or omission that is unlawful or intended to circumvent the law with respect to the provisions referred to in clause 3.1 of the Rules;

2.7. Follow-up Actions – any actions necessary to investigate the Report, examine the circumstances described therein, including assessing the authenticity of the allegations contained therein, determine whether a Breach has occurred, and, if a Breach is found to have occurred, take steps to ensure an appropriate and adequate response to the Breach;

2.8. GDPR – 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;

2.9. Records of Reports – the Records of Reports referred to in clause 8 of the Rules;

2.10. Report – the communication of information to the Company on an act or omission intended to circumvent the law or regulations referred to in clause 3.1 of the Rules;

2.11. Reporting Channel – a dedicated email box at the following address: sygnalisci@controlant.com, as referred to in clause 6.1 of the Rules;

2.12. Retaliation – any act or omission that is repressive in nature and occurs in response to a Report, and in particular any acts or omissions that contribute or may contribute (directly or indirectly) to the deterioration of the legal or factual situation of a Whistleblower or a person connected with them (in particular a relative, a family member, or a co-worker), including any acts adversely affecting the conditions of their work or employment. Any threats and attempts to engage in Retaliation will be treated in the same way as actual Retaliation;

2.13. Rules – these Rules as amended from time to time;

2.14. Whistleblower – any natural person referred to in clause 3.2 of the Rules;

2.15. Whistleblower Contact – persons holding at the Company the positions of "Head of HR" and "HR Manager-Poland", who are designated by the Company as responsible for receiving Reports under these Rules.

3. THE SCOPE OF APPLICATION OF THE RULES

3.1. These Rules apply to Reports concerning a breach of the law consisting of an act or omission that is unlawful or intended to circumvent the law, relating to:

a) corruption;
b) public procurement;
c) financial services, products and markets;
d) prevention of money laundering and terrorist financing;
e) product safety and compliance;
f) transport safety;
g) protection of the environment;
h) public health;
i) consumer protection;
j) protection of privacy and personal data;
k) security of network and information systems;
l) financial interests of the State Treasury, local government units or European Union
m) the internal market of the European Union, including competition and State aid rules under public law, as well as corporate tax;
n) other areas set out in Art. 3(1) of the Act,

("Breach").

3.2. Within the meaning of these Rules, Whistleblowers are defined as natural persons who report a Breach in a work-related context, including employees, temporary employees, individuals performing work on a basis other than employment, including under a civil law contract, entrepreneurs, commercial proxies, shareholders, members of a body of the Company, individuals working under the supervision and direction of the Company's contractor, subcontractor or supplier, trainees, volunteers and interns, as well as natural persons applying for employment (or seeking to establish any other legal relationship serving as a basis for performing work or providing services or holding office) with the Company, or persons whose employment (or any other legal relationship serving as a basis for performing work or providing services or holding office) has already ended ("Whistleblower").

1. WHISTLEBLOWER PROTECTION

1.1. It is prohibited for the Company (including its employees and other persons performing activities for the Company) to commit any acts of Retaliation against a Whistleblower who made a Report in good faith. This prohibition will apply accordingly to a person who assists the Whistleblower in making such a Report and to a person otherwise connected with the Whistleblower (in particular, a relative, a family member or a co-worker).

1.2. If an employee commits an act of Retaliation, this will constitute a grave breach of their basic employee duties and may give rise to legal consequences for such an employee resulting from the applicable laws, including penalties for breach of order and discipline provided for in labour laws or the termination of the employment contract with such an employee. The preceding sentence will apply accordingly to acts of Retaliation by persons performing activities for the Company on a basis other than a contract of employment.

1.3. A Whistleblower is deemed to have made a Report in good faith if they had reasonable grounds to believe that the information concerning the Breach:

1.1.1. was true at the time of making the Report,
1.1.2. related to a Breach of the regulations set out in clause 3.1 of the Rules.

1.4. If a Whistleblower had reasonable grounds to believe that the Report was necessary to reveal a Breach of the regulations set out in clause 3.1, they may not suffer Retaliation. Otherwise, if, as a result of the Follow-up Actions, it is found that the person making the Report has knowingly and intentionally made a false Report, such action may be considered as a grave breach of employee duties, and in the case of a person performing work under another contract, the contract may be terminated for reasons attributable to the person performing work.

1.5. Forms of Retaliation may in particular include:

1.1.1. refusal to enter into an employment or other legal relationship under which work was to be performed;
1.1.2. termination of a contract of employment or any other contract between the Whistleblower and the Company;
1.1.3. failure to renew a contract of employment or any other contract between the Whistleblower and the Company concluded for a fixed term and convert it into a contract for an indefinite period in a situation where the Whistleblower could have had an objective and reasonable expectation that it would be renewed;
1.1.4. demotion or withholding of promotion;
1.1.5. unfavourable change in the conditions of work or pay, and specifically: transfer of duties to another person, change in location of place of work or change in working hours, reduction in remuneration, limitation or withholding of benefits other than remuneration;
1.1.6. withholding or limitation of training;
1.1.7. negative performance assessment or employment reference;
1.1.8. imposition of penalties for breach of order and discipline (warning, reprimand or fine) or any other disciplinary measure;
1.1.9. any pressure, intimidation, ostracism or bullying;
1.1.10. discrimination, disadvantageous or unfair treatment;
1.1.11. causing any harm (including to the person's reputation) or financial loss, including loss of business and loss of income;
1.1.12. blacklisting the Whistleblower on the basis of a sector or industry-wide informal or formal agreement that may result in the person not finding employment in a particular sector or industry in the future;
1.1.13. taking steps intended to result in the cancellation of the Whistleblower's licence, permit or any other document confirming the Whistleblower's professional qualifications or certification;
1.1.14. unwarranted psychological or medical referral (including psychiatric one);
1.1.15. termination of a contract of employment or any other contract under which the Whistleblower performs work, in particular a contract for the sale or supply of goods or provision of services, as well as withdrawal from such a contract or its termination without notice;
1.1.16. imposition of an obligation, refusal to grant a right, or limitation or withdrawal of a right.

1.6. Notwithstanding the provisions of clause 4.5 above, actions that are warranted on objective grounds or by law, as well as actions that are not connected with the Report are not considered to be Retaliation.

1.7. Irrespective of the prohibition referred to in clause 4.1 above, the Company undertakes to ensure that the Whistleblower suffers no Retaliation by the employees or persons performing activities for the Company or by third parties (including, in particular, employees or other persons performing activities for the other companies from the Controlant Group). To this end, the Company, in particular:

1.1.1. enables the employees and other persons performing activities for the Company to make Reports of Retaliation against them, also through the Reporting Channel;
1.1.2. undertakes to take necessary and reasonable steps to hold legally accountable those employees, persons performing activities for the Company and third parties (including, in particular, employees or other persons performing activities for the other Companies from the Controlant Group) who commit or attempt to commit acts of Retaliation;
1.1.3. provides, as far as possible, appropriate and adequate assistance to the person suffering Retaliation, in particular as regards reporting acts of Retaliation committed by third parties to the competent authorities.

2. CONFIDENTIALITY AND ANONYMITY

2.1. All persons with access to Confidential Information are obliged:

1.1.1. not to disclose or provide the Confidential Information to any third party;

1.1.2. to take any necessary precautions to prevent a disclosure of the Confidential Information;

1.1.3. to use the Confidential Information only for the purposes of handling the Reports, operating the Reporting Channel, taking Follow-up Actions, or responding to an identified Breach;

1.1.4. to exercise due care and diligence in protecting the Confidential Information from unauthorised access by third parties, in particular by duly complying with the procedures for protecting the Confidential Information in place at the Company, and by duly applying the safeguards implemented by the Company, in accordance with the provisions of the following clauses.

2.2. The Company enables Whistleblowers to make Reports anonymously. Irrespective of whether a Whistleblower has exercised their right to make a Report anonymously, their identity constitutes Confidential Information. A Whistleblower may at any time waive their right to be anonymous or to keep their identity confidential.

2.3. A Whistleblower who intends to make a Report anonymously should make the Report using:

1.1.1. a device that does not belong to the Company and is not a part of the Company's IT infrastructure,

1.1.2. access to the Internet through an access point that is not maintained by the Company,

1.1.3. an email address other than the Whistleblower's company email address or any other email address communicated to the Company, set up in a manner that prevents direct or indirect identification of the Whistleblower (in particular an address that does not contain the Whistleblower's surname, initials or a commonly known pseudonym).

2.4. The Company undertakes to protect the identity of the Whistleblower as well as any information and documents relating to the Report or coming from the Whistleblower on the basis of which the identity of the Whistleblower can be directly or indirectly deduced. It is prohibited for the Company (or its employees or any persons performing activities for the Company) to take any action with the purpose of discovering or disclosing the identity of the Whistleblower who has made a Report anonymously.

2.5. Access to the Confidential Information is only granted to the Whistleblower Contact and members of the Company's Management Board. The Company shall grant to any persons having access to the Confidential Information a separate written authorisation (except for the Management Board Members for whom such authorisation is not required). The Company undertakes to secure the Reporting Channel and the Records of Reports using available adequate technical and organisational measures to prevent access by persons other than those listed in this clause.

2.6. The Company may only disclose the Confidential Information in the event that:

1.1.1. it has been disclosed to the public by the Whistleblower or by a third party without breaching the Rules or the applicable laws;

1.1.2. the disclosure is a necessary and proportionate step needed to take Follow-up Actions or to respond to an identified Breach;

1.1.3. it has to be disclosed to the competent public authorities in accordance with the applicable laws or pursuant to an enforceable ruling.

The provisions of clauses 5.6.1. and 5.6.2. do not, in any case, apply to the disclosure of the Whistleblower's identity or any information on the basis of which the identity of the Whistleblower can be directly or indirectly deduced. If only a part of the Confidential Information falls under one of the exceptions set out in clauses 5.6.1. to 5.6.3., the provisions of clause 5.1. will continue to apply to the rest of such Confidential Information.

3. THE REPORTING CHANNEL AND THE REPORTING PROCEDURE

3.1. For the purpose of making Reports in writing, the Company has set up a dedicated email box at the following address:

sygnalisci@controlant.com

(“Reporting Channel”).

3.2. The Whistleblower Contact is responsible for operating the Reporting Channel and for receiving Reports. The members of the Company’s Management Board also have the authority to access the Reporting Channel, but they are not responsible for operating the Reporting Channel.

3.3. It is prohibited for persons who have access to the Reporting Channel to:

1.1.1. forward a Report, including creating automated orders to forward the Reports,

1.1.2. print the content of a Report or the documents attached to it,

1.1.3. copy the content of a Report or the documents attached to it, make transcriptions and recordings in electronic or paper form, including taking photographs, taking screenshots or taking any other action with the purpose of reproducing the content of a Report or the documents attached to it.

The aforementioned prohibitions do not apply in a situation where such an obligation arises under the Act or the Rules or where it is a necessary and proportionate step needed in order to take Follow-up Actions or respond to an identified Breach, as well as with respect to a Report referred to in clause 4.4, last sentence.

3.4. The Reporting Channel:

1.1.1. is intended solely for the receipt of Reports and communication with the Whistleblower and must not be used for any other communication,

1.1.2. ensures the confidentiality, integrity, availability and accountability of the information, including its proper protection against unauthorised or accidental destruction, loss, modification, unauthorised disclosure or access,

1.1.3. ensures the full anonymity of the Whistleblower in the event the Reports are made anonymously,

1.1.4. enables the Reports as well as the information contained in them and the documents attached to them to be stored in a manner that ensures that Follow-up Actions are taken.

3.5. A Report shall include, in particular:

1.1.1. a concise description of the case, including a description of the Breach,

1.1.2. identification of the person or organizational unit that the Report concerns,

1.1.3. identification of the Breach of the regulations referred to in clause 3.1.

3.6. Optionally, a Report may include:

1. the source of the Whistleblower's knowledge of the Breach,
2. identification of the person or persons who have witnessed the Breach or who have or may have knowledge of the Breach,
3. a description of other facts and circumstances that may be relevant to the determination that the Breach has occurred and to Follow-up Actions,
4. Whistleblower’s contact details.

3.7. After a Report has been made, the Whistleblower Contact is obliged to confirm to the Whistleblower the acceptance of the Report **within no more than 7 days** of the date the Report was made, to the email address from which the Report was sent.

3.8. The Whistleblower Contact shall treat all Reports objectively and impartially, and with respect for the rights of the persons that the Report concerns,

3.9. The Management Board of the Company is obliged to take Follow-up Actions with due care and diligence, as appropriate to the circumstances of the case. The Management Board may also appoint by the means of the resolution one or more members of the Management Board to take Follow-up Actions on behalf of the Company. The Follow-up Actions may include, in particular:

1.1.1. verification of the Report,

1.1.2. further communication with the Whistleblower, as well as a request for additional information from the Whistleblower and provision of feedback to the Whistleblower,

1.1.3. rejection of the Report in cases where the Report:

a. is manifestly unfounded, or
b. clearly does not relate to a Breach of the regulations set out in clause 3.1 of the Rules,

1.1.4. initiation of an investigation or internal enquiry,

1.1.5. consultation with external or internal advisors (i.e. within the Controlant Group) in compliance with the rules regarding confidentiality and anonymity,

1.1.6. closure of the investigation or internal enquiry due to lack of sufficient information or evidence, or due to a determination that no Breach has occurred,

1.1.7. determination that a Breach has occurred.

3.10. In the event that a Breach is found to have occurred, the Company's Management Board will take measures and actions ensuring appropriate and adequate response to the Breach, depending on its nature and the circumstances of the case, such as in particular:

1.1.1. steps designed to remedy the effects of the Breach, in particular by taking actions that are in compliance with the applicable laws or refraining from actions that are not in compliance with the applicable laws,

1.1.2. preventive actions intended to ensure that similar Breaches do not occur in the future, in particular by implementing appropriate procedures, taking specific measures to raise awareness, carrying out additional training for the employees, or implementing specific technical or organisational solutions,

1.1.3. legal and disciplinary measures against the person who committed the Breach,

1.1.4. notification to the competent authorities if there is a suspicion that the Breach constitutes a misdemeanour, an criminal offence, a criminal and fiscal offence, or an administrative tort,

1.1.5. assistance provided to the person adversely affected by the Breach.

3.11. The Management Board of the Company will provide feedback to the Whistleblower on the Follow-up Actions as well as on the measures that have been or are to be taken in response to the identified Breach, within a maximum period of 3 months from the date of confirming the receipt of the Report.

3.12. The Management Board of the Company will carry out the actions provided for in the Rules, including making a decision on the Follow-up Actions, on the basis of the provisions of these Rules and generally applicable laws, objectively and impartially and with respect for the rights of the persons that the Report concerns.

3.13. In the event of a Report concerning a person being a member of the Company's Management Board, a decision on the Follow-up Actions will be made by other members of the Management Board.

4. PERSONAL DATA

4.1. The processing of personal data of the Whistleblower, the connected persons and other persons who are identified in the Report (or who can be identified on the basis of the Report) is carried out to the extent necessary for handling the Reports and taking Follow-up Actions in relation to the Reports or proceedings initiated by such Actions, on the basis of Article 6(1)(c) of the GDPR – i.e. processing is necessary for compliance with legal obligations to which the Company is subject in connection with the obligation to establish the Internal Reporting Rules under the Act and to accept Reports and take Follow-up Actions.

4.2. A Report should not contain the special categories of personal data referred to in Article 9(1) of the GDPR, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or genetic data, biometric data, or data concerning health, sex life or sexual orientation or in Article 10 of GDPR, i.e. data relating to criminal convictions and offences or related security measures.

4.3. A Report should not contain the personal data that are not relevant for the handling of a Report.

4.4. A privacy notice concerning the processing of personal data is attached as an Appendix to these Rules.

4.5. The personal data processed in connection with the acceptance of a Report or with the Follow-up Actions as well as the documents relating to such a Report will be retained by the Company for a period of three years following the end of the calendar year in which the Follow-up Actions were

completed or following the end of the proceedings initiated by such Actions. After the end of the aforesaid period, they will be deleted and destroyed.

4.6. The preceding sentence applies accordingly to the personal data and other information stored in the Records of Reports.

4.7. The Whistleblower Contact will review the personal data processed by the Company under the Rules no less frequently than once a calendar year in order to determine if their continued retention is necessary. The Company will delete the personal data whose continued retention is not necessary for the purpose set out in the Rules.

5. RECORDS OF REPORTS

5.1. The Whistleblower Contact maintains Records of the received Reports in electronic form **("Records of Reports")**.

5.2. The Records of Reports contain the following data:

1.1.1. the number of the Report,

1.1.2. the date on which the Report was made,

1.1.3. the personal data of the Whistleblower (provided the Whistleblower has not made the Report anonymously) and the person that the Report concerns, necessary to identify those persons,

1.1.4. the Whistleblower's contact address,

1.1.5. the subject matter of the Breach,

1.1.6. information on the Follow-up Actions taken,

1.1.7. the date on which the case was closed.

5.3. Notwithstanding the Records of Reports, the Company retains the document or other data storage medium containing the Report or attached to the Report.

6. EXTERNAL REPORTING

6.1. A person who has reasonable suspicion of an act or omission that is unlawful or is intended to circumvent the law, as referred to in clause 3.1. of the Rules, may, notwithstanding the provisions of these Rules, make External Report and notify the competent public authorities, the Ombudsman or entities, bodies or institutions of the European Union.

6.2. External Report can be made to:

9.2.1. any relevant public authority (local or central), relevant for the matter, depending on the subject of the report; Each public authority is required to publish detailed information on its Public Information Bulletin (Polish: *Biuletyn Informacji Publicznej - BIP*) website about the procedure for submitting External Reports, including the scope of matters that can be reported to that specific authority;

9.2.2. Ombudsman (Polish: *Rzecznik Praw Obywatelskich*);

- Detailed information for Whistleblowers intending to make External Report to Ombudsman: https://www.gov.pl/web/sygnalisci
- The procedure for submitting External Reports to Ombudsmen: https://bip.brpo.gov.pl/sites/default/files/2024-12/Zarzadzenie_67_2024_RPO_procedura_zgloszen_zewnetrznych_w_BRPO.pdf
- The dedicated website for making External Report to Ombudsman: https://sygnalisci.brpo.gov.pl/pl

7. FINAL PROVISIONS

7.1. The Rules will come into force on August 8, 2025.

7.2. The representatives of the persons performing work for the Company has been consulted on these Rules in accordance with the procedure set out in Art. 24(3) and (4) of the Act.

PRIVACY NOTICE

pursuant to Articles 13 and 14 of the GDPR in relation to the processing of a whistleblower's personal data and personal data obtained from a person other than the data subject

5. **Controlant Poland Spółka z ograniczoną odpowiedzialnością** with its registered office in Wroclaw (50-082), at 1 ks. Piotra Skargi Street, entered in the register of entrepreneurs maintained by the District Court for Wrocław-Fabryczna in Wrocław, 6th Commercial Division of the National Court Register, under KRS No.: 0000927230, is the personal data **Controller**; email address for matters relating to the processing of personal data in connection with reports: sygnalisci@controlant.com.
6. Personal data are processed on the basis of:
   - Article 6(1)(c) 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) (OJ EU L of 2016 No. 119, p. 1, as amended) – hereinafter referred to as "GDPR" – i.e. the processing is necessary for compliance with the Controller's legal obligations in connection with the obligation to establish an internal reporting procedure under the Whistleblower Protection Act of 14 June 2024 (Journal of Laws, item 928) and to receive reports and take follow-up actions,
   - Article 9(2)(g) of the GDPR in connection with the provisions of the Whistleblower Protection Act, if such personal data are included in the whistleblower's report and are necessary to receive the report or take follow-up actions.
7. The purpose of the processing of personal data is to take steps in order to determine whether the reported act or omission constitutes an actual or potential breach and, if necessary, to take follow-up actions and respond to such a breach.
8. The scope of the personal data that are processed includes: the name of the whistleblower, the name of the persons indicated in the report, contact details such as the telephone number, email address and/or mailing address of the whistleblower, and, where applicable, contact details of persons whose data have been provided in the report.
9. Personal data that are not relevant to the report are not collected. If, however, they are collected by accident, they are deleted immediately, but no later than 14 days after it is established that they are not relevant to the case.
10. Personal data may be made available only to entities authorised to process them under the law. In addition, on the basis of agreements entered into by the Controller, personal data will be made available to external entities responsible for or supporting the operation of the internal reporting system or providing support to the Controller with respect to any follow-up actions.
11. Personal data may be transferred to the external entities referred to in clause 6 to third countries, including those not providing an adequate level of protection. In such an event, personal data are transferred to entities that are obliged to ensure an adequate level of protection of personal data, e.g. by applying standard contractual clauses approved by the European Commission. However, in the event that personal data are transferred from the EEA to organisations that have signed up to the EU-US Data Privacy Framework, this is possible without the need to obtain additional authorisations or use legal instruments such as standard contractual clauses or binding corporate rules. [1]
12. The Controller does not take automated decisions (in particular through profiling) when handling or processing reports.
13. Data subjects have the right to request from the Controller access to personal data, their rectification or erasure, or restriction of their processing, the right to object to the processing, as well as the right to data portability, with the proviso that those rights may be subject to limitations set out in the applicable laws (including the GDPR). The provisions of Articles 14(2)(f) and 15(1)(g) of the GDPR do not apply, i.e. the Controller does not disclose the source of personal data (the identity of the whistleblower or any other data that may directly or indirectly reveal the identity of the whistleblower) unless the whistleblower has consented to it or the person making the report does not have the status of a whistleblower within the meaning of the Whistleblower Protection Act.
14. Personal data processed in connection with the receipt of a report or with the follow-up actions and documents relating to such a report as well as information contained in the records of reports

will be retained by the Controller for a period of 3 years following the end of the calendar year in which the follow-up actions were completed or following the end of the proceedings initiated by such actions.

15. The data subject has the right to file a complaint with the President of the Personal Data Protection Authority.
16. The provision of his/her personal data by the whistleblower in the report is voluntary.
17. In the event that the Controller is not able to identify the data subject (in particular with regard to a whistleblower who has exercised his/her right to make a report anonymously), such data subject will not have the right to request from the Controller access to personal data, their rectification or erasure, or restriction of their processing as well as the right to data portability, unless the data subject, in order to exercise the aforementioned rights, provides additional information allowing him/her to be identified.