



Group Whistleblowing Policy

	Name	Position	Date
Issued by:	Rohia Hakimová	Group AML & Compliance Officer	07 January 2025
Approved by:	Richard J. Wilkinson	Group CFO	08 January 2025
	Alexander Klein	Group Deputy CFO	09 January 2025
	Peter Čerešník	Group COO	10 January 2025

Version number:	02
Effective date:	15 January 2025
Date and place of Issue:	13 January 2025, Prague
Applicable to:	Everyone, both within the CTP Group and external third parties involved in a work-related context with the CTP Group or any of its member companies, is encouraged to report any suspected misconduct or irregularity.

Previous versions overview	
01	Group Whistleblower Policy 29 March 2021

1. INTRODUCTION

- 1.1 The CTP group companies (the "**CTP Group**" or "**we**") is committed to conduct business at all times in compliance with all applicable laws and regulations and all of the CTP Group's codes and policies. Therefore, it is important that the CTP Group is aware of all possible violations, especially those that violate applicable laws and legal regulations, including but not limited to applicable anti money-laundering laws and regulations, (together the "**Legislation**") our Code of Conduct or other CTP Group's policies.
- 1.2 Any reference made to the CTP Group further in this whistleblower policy (the "**Policy**") shall include any CTP Group entity.
- 1.3 This Policy is intended to encourage everyone, both within the CTP Group and outside to third parties, who are involved in a work-related context with the CTP Group or any of its member companies ("**you**") to report any suspected misconduct or irregularity. This Policy sets out what and how matters should be reported, the main principles of the procedure to be followed once a report has been made, and how persons reporting their concerns are protected and applies to both our employees and other Whistleblowers, e.g. employees of third parties and as further defined below.
- 1.4 This Policy is prepared under the direct instruction of the board of the CTP Group (the "**Board**"). This Policy and other materials about reporting your concerns are published on the CTP Group's website and intranet.
- 1.5 In the event of any conflict between this Policy and applicable Legislation, the provisions of the Legislation will take precedence. This Policy applies to all members of the CTP Group, but due to different local legal requirements, we have created annexes or separate local policies to address specific needs. Where there's a difference, the local annex or policy will take priority to ensure full compliance with national regulations.

2. WHO CAN REPORT?

- 2.1 **Any individual**, including external parties, who has acquired information on Breaches (as defined below in paragraph 3.1) in the **work-related context**¹ may submit a report. This includes especially:
- employees;
 - self-employed persons (individual contractors);
 - shareholders and members of CTP Group's bodies, including non-executive members;
 - volunteers;
 - paid or unpaid trainees;
 - persons working under the supervision and direction of contractors, subcontractors and suppliers.

¹ 'Work-related context' means current or past work activities through which, irrespective of the nature of those activities, persons acquire information on Breaches and within which those persons could suffer retaliation if they reported such information.

all of the above **including applicants** for the aforementioned positions and **individuals who held these positions in the past**.

An individual who makes a report via global or local whistleblowing channels or who publicly discloses² information on Breaches acquired in the context of his or her work-related activities is called whistleblower (the "**Whistleblower**").

3. WHICH CONCERNS ARE COVERED BY THIS POLICY?

3.1 This Policy can be used to report information, including reasonable suspicions, about actual or potential breaches (the "**Breaches**"), which occurred or are very likely to occur in the CTP Group, and about attempts to conceal such Breaches.

3.2 The Breaches mean acts or omissions that represent or may represent a violation or encouragement to violate human rights, the Legislation, rules, values, and principles established by the CTP Group's policies.

3.3 For **example**, the following Breaches should be reported:

- Fraud, bribery and corruption;
- Violations of competition law;
- Failure to comply with a legal obligation;
- Incidents in protection of confidential information and insider trading;
- Incidents in protecting the CTP Group's assets, data and information;
- Inadequate financial or non-financial record keeping;
- Conflicts of interests;
- Health & Safety, Security and Environment issues;
- Improper use of the CTP Group's resources;
- Violations of our policies on gifts and hospitality;
- Any kind of discrimination – due race, nationality or ethnicity, gender, education, age, religion, political preferences, sexual orientation, personal status or disability, any kind of harassment or abuse;
- Breaches of the EU acts in the area of: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data, and security of network and information systems; Breaches affecting the financial interests of the EU; breaches relating to the internal market, including breaches of EU competition and state aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

² 'Public disclosure' or 'to publicly disclose' means the making of information on Breaches available in the public domain. For more information see paragraph 8.2 to this Policy.

3.4 You are encouraged to raise any other concern by using this Policy if you feel this is appropriate, even if your concern is not listed above.

4. WHO AND HOW SHOULD I REPORT TO?

Reporting on the Local Level

4.1 Every single entity of the CTP Group has established whistleblowing channels and appointed appropriate persons in accordance with EU and relevant local legislations to receive whistleblowing reports and follow-up on them (the “**Designated Persons**”).

4.2 The whistleblowing channels enable reporting **in writing or orally via hot line**. Upon your request, the report can be made also by means of an **in-person meeting with the Designated Person**, which shall take place within a reasonable timeframe after the request is made.

4.3 When reporting through the local whistleblowing channel, you have the following options:

- **Whistleblowing platform:** more information is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).
- **Post mail:** postal item to be sent to the address of the respective CTP Group entity, to the attention of the respective Designated Person (**do not forget to include the name of the Designated Person on the envelope!**)
- **Hot line:** the phone number for the hotline for individual CTP Group entities is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).
- **In-person meeting:** please, contact the Designated Person for your CTP Group entity.
- **E-mail to the Designated Persons:** use the email address specifically designated for receiving whistleblowing reports, available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).

Reporting on the Global Level

4.4 In addition to the local whistleblowing channels, a group-wide whistleblowing channel has been established at the CTP Group global level. You are **free to choose** which channel (whether local or global) to use based on your preference. You should bear in mind that the local channels are designed to ensure compliance with local laws. The global channel and the subsequent internal investigation process may not correspond to particular local legal requirements. You are encouraged to consider these factors when deciding the most appropriate channel for their reports.

4.5 When reporting through the global whistleblowing channel, you have the following options:

- **Whistleblowing platform:** more information is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).

- **E-mail address:** whistleblowing@ctp.eu
- **Post mail:** CTP Invest, spol. s r.o., Attn: Group AML & Compliance Officer, Národní 135/14, 110 00 Prague, Czech Republic.
- **Hot line:** (+420) 607 287 287.
- **In-person meeting:** please, contact the Group AML & Compliance Officer (the contact details can be found on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>)).

Reporting Grievances – Global and Local Channels

4.6 Instead of using our designated whistleblowing channels, you are **free to choose** to use grievance reporting channels both on local and global level for reporting certain matters. These channels are specifically designed for addressing grievances, i.e. discrimination, any form of harassment including sexual harassment and ESG concerns.

4.7 The global grievance channel provides equal level of protection and operates on the same principles as a global whistleblowing channel. Local grievance channels provide similar protection and operate on the similar principles as local whistleblowing channels. The grievance channels are standalone reporting channels separate from the whistleblowing channels, which are regulated by law. The grievance channels are not operated by the Designated Persons and by design they do not have to meet such strict legal standards which are typical for whistleblowing. You are encouraged to consider these factors when deciding the most appropriate channel for your report.

4.8 More information on grievance channels can be found on the intranet (<https://intranet.ctp.eu/web/guest/grievance>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).

Sharing a Concern with Managers and Executive Committee Members

4.9 If you are comfortable doing so, you are encouraged to first share your concern with your manager, if applicable (that is, if you are a person who has a manager within the CTP Group). If the suspicion relates to an Executive Director of the Board, you can share your suspicions directly with the Non-Executive director of the Board, whose name and contact details are available on the CTP website.

4.10 While you can report your concerns to the people listed above in paragraph 4.9, please remember that **they are not the official Designated Persons for handling such reports** and this Policy does not cover the procedures for when you share your concerns with them.

5. WHAT SHOULD THE REPORT CONTAIN?

5.1 When raising a concern in writing, you should consider the person reading it will not know anything about the issue. You should provide as much details as possible. The whistleblowing channel is anonymous, however providing name and contact details of the Whistleblower will help to get more details if necessary and improve the investigation.

5.2 For a proper investigation of the suspected Breach, it is advisable that the report contains at least the following basic information:

- (i) details about the concern – background, history and reason;
- (ii) name(s) and surname(s) of the person(s) concerned³;
- (iii) name(s) and surname(s) of witness(es);
- (iv) date, time and place of the incident(s);
- (v) details of any evidence;
- (vi) affected funds or other assets;
- (vii) any supporting documentation available;
- (viii) how often the incident has occurred.

6. CAN I REMAIN ANONYMOUS?

6.1 The CTP Group encourages an open culture and emphasizes the importance of raising any concerns openly to assess, investigate and gather additional information, if needed.

6.2 If the Whistleblower raises concerns openly, the CTP Group will use all reasonable efforts to ensure the Whistleblower's identity will not be revealed without the Whistleblower's previous written consent (unless the CTP Group is required to comply with the Legislation) and treat the report confidentially according to the rules set in Article 9. However, if you do not wish to openly raise concerns, you can report anonymously by using both global and local whistleblowing and grievance channels.

6.3 The Whistleblowers who reported or publicly disclosed information on Breaches anonymously, but who are subsequently identified, shall be protected under this Policy, provided that they meet the conditions laid down in Article 8 of this Policy.

7. WHAT HAPPENS AFTER I REPORT A CONCERN?

7.1 The CTP Group takes every report of suspicions of possible Breaches seriously. All reports delivered via designated global or local whistleblowing channels will be dealt with fairly, properly and without undue delay.

7.2 If the Whistleblower has provided a secure and reliable means of communication⁴, he/she will be acknowledged of receipt of the report within 7 days from the date of its receipt.

³'Person concerned' means a person s a natural or legal person who 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.

⁴The use of a generic e-mail account, to which more than one user may have access (for example, construction@ctp.eu) shall not be considered neither secure nor reliable.

7.3 The CTP Group is committed to provide the Whistleblower with a thorough follow-up. This means we will inform the Whistleblower about the actions we plan to take or have taken, and explain the reasons for those actions.

7.4 However, the need for confidentiality and privacy and other legal obligations may prevent the CTP Group from being able to give the Whistleblower (specific) details regarding the investigation or actions taken. Any information shared with the Whistleblower about the investigation and action taken must be treated as confidential.

7.5 The CTP Group will give feedback to the Whistleblower within a reasonable time, which will be no more than three months from when we acknowledged receiving the report. If we didn't send an acknowledgment, we will provide feedback within three months from the end of the seven-day period after the report was submitted.

7.6 The CTP Group cannot guarantee the outcome expected or desired by the Whistleblower. However, the CTP Group is committed to deal with the Whistleblower's genuine concerns fairly and appropriately.

8. WHO IS PROTECTED UNDER THIS POLICY?

8.1 The Whistleblowers shall qualify for protection under this Policy provided that all of these conditions are met at the same time:

- (a) **They reported in good faith.** Whistleblowers will not be protected under this Policy if they did not have reasonable grounds to believe that the information reported was true at the time. However, you do not need to be certain that a Breach has taken place in order to speak up.
- (b) **They had reasonable grounds to believe that the information on Breaches reported was relevant to this Policy.**
- (c) **They reported via designated channels** (i.e., internally via global or local whistleblowing channels or global or local grievance channel or externally in accordance with Article 12 and respective annexes to this Policy) **or made a public disclosure (see paragraph 8.2).**

Public disclosure

8.2 You will be protected under this policy if you share information publicly and any of the following conditions are met:

- a) You reported the issue both internally and externally (or just externally), but no appropriate action was taken within: (i) three months from when we acknowledged receiving the report, or within three months from the end of the seven-day period after the report was submitted if no acknowledgment was sent (for internal reports) or (ii) within a reasonable time, not exceeding three months or up to six months in duly justified cases for external reports), or
- b) You have good reasons to believe that:
 - the issue poses an immediate or obvious danger to public interest (e.g. emergency or irreversible damage), or
 - in the case of external reporting, there is a risk of retaliation, or a low chance the issue will be effectively handled. This could be because evidence might be hidden or

destroyed, or because the authority involved is not trustworthy or is connected to the problem.

This rule does not apply if someone directly shares information with the press according to national laws that protect freedom of speech and information.

9. HOW MY IDENTITY WILL BE PROTECTED AND WILL THE REPORTS BE TREATED CONFIDENTIALLY?

9.1 The CTP Group will treat any report confidentially in order to allow for an adequate investigation of the report and to comply with the Legislation including privacy laws.

Protection of the identity of the Whistleblower

9.2 The identity of the Whistleblower will not be disclosed to anyone beyond the Designated Persons, without the explicit prior written consent of the Whistleblower. The Whistleblower is entitled to deny or withdraw his or her consent at any time and must be informed of this right prior to giving consent. This shall also apply to any other information from which the identity of the Whistleblower may be directly or indirectly deduced (e.g. work position, birth date etc.).

9.3 There are exceptions to paragraph 9.2. The identity of the Whistleblower and other information mentioned in paragraph 9.2 may be shared if required by EU or national law for investigations or court cases. This can also happen to protect the rights of the person concerned. Whistleblowers will be notified in written before their identity is revealed, unless it would harm the investigation or court case. When notifying the Whistleblowers, they will receive a written explanation of why their confidential information is being shared.

Other confidential information

9.4 The other information received (without prejudice to the paragraphs 9.1, 9.2 and 9.3) will only be shared with others within or outside the CTP Group if and to the extent this is required to appropriately deal with the report and the issues raised in it and in accordance with the Legislation.

9.5 The CTP Group will generally notify the person implicated in a report that concerns have been raised in relation to him or her unless it could jeopardize the proper follow-up or there were other justifiable reasons for it. The CTP Group will make this notification within a reasonable time and take into consideration the interests of the investigation. The CTP Group will take all reasonable measures to prevent the person implicated in a report from learning the identity of the Whistleblower.

9.6 If it turns out the report was not made in good faith, the CTP Group is not bound by these confidentiality obligations, with the exception of applicable privacy laws.

10. HOW WILL I BE PROTECTED AGAINST RETALIATION IF I REPORT A CONCERN?

10.1 Retaliation is any direct or indirect action or failure to act in a work-related setting that happens because of internal or external reporting, or public disclosure as per this Policy. It results in or can result in unfair harm to the Whistleblower.

10.2 No Whistleblower who in good faith raises a concern involving matters covered by this Policy will suffer retaliation as a result of raising a concern. The CTP Group is committed to protect the Whistleblowers submitting disclosures in good faith against retaliation. All Whistleblowers will be treated with respect, dignity and confidentiality.

10.3 Retaliation within this Policy includes threats of retaliation and attempts of retaliation including in particular in the form of:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in wages, change in working hours; (d) withholding of training;
- a negative performance assessment or employment reference;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

10.4 The measures for the protection of the Whistleblowers set out in this Article 10 shall also apply, where relevant, to:

- Facilitators (meaning a natural person who assists a Whistleblower in the reporting process in a work-related context, and whose assistance should be confidential);
- third persons who are connected with the Whistleblowers and who could suffer retaliation in a work-related context, such as colleagues or relatives of the whistleblowers; and
- legal entities that the Whistleblowers own, work for or are otherwise connected with in a work-related context.

11. CAN I ASK SOMEONE FOR ADVICE?

11.1 Members of our staff are free to choose to consult their manager about suspicions of a possible Breach. If you will not find an answer, or prefer to or simply cannot consult your manager (for example if the suspicion relates to him or her), you can consult the Group AML Compliance Officer. The contact details of the Group AML Compliance Officer can be found on the intranet. Please, bear

in mind that sharing your concern in this manner is not considered whistleblowing under this Policy, unless one of these individuals is also a Designated Person.

12. CAN I REPORT CONCERNS OUTSIDE THE CTP GROUP?

12.1 You are encouraged to report your concerns internally. As the CTP Group operates in several jurisdictions, different rules may apply concerning circumstances under which certain specific suspicions can be reported outside the CTP Group. We refer to Annexes to this Policy pertaining to individual CTP Group entities for more information.

13. PROCESSING OF PERSONAL DATA

13.1 Any processing of personal data carried out pursuant to this Policy, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680.

13.2 Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.



Annex AUSTRIA

1. INTRODUCTION

- 1.1 Main legal basis with regard to whistleblowing in Austria is the Austrian Whistleblower Protection Act (*Hinweisgeberschutzgesetz* – “HSchG”), implementing the EU Whistleblowing Directive on local level. The HSchG legally protects Whistleblowers as defined in Section 2 of the Policy, but only regarding breaches of the EU acts as stated in Section 3.3 of the Policy as well as their local implementing laws and breaches regarding fraud, bribery and corruption according to Sections 302 to 309 of the Austrian Criminal Code (*Strafgesetzbuch* – “StGB”).
- 1.2 This Annex serves as addition to the Group Whistleblower Policy (the “Policy”) and contains specific local provisions regarding the Austrian entities and applying to all individuals stated in Section 2 of the Policy and only insofar the HSchG is applicable.
- 1.3 All other provisions are voluntary extensions by CTP and remain unaffected by this Annex.

2. SPECIFIC LOCAL PROVISIONS DEVIATING FROM THE POLICY

- 2.1 **In-person meetings according to Section 4.2 of the Policy:** In case you want to make a report by means of an in-person meeting with the Designated Person, such meeting shall take place within 14 calendar days after the request is made.
- 2.2 **Feedback period according to Section 7.5 of the Policy:** The CTP Group will give feedback to the Whistleblower within a reasonable time, which will be no more than three months after the report was submitted.
- 2.3 **Public disclosure according to Section 8.2 of the Policy:** You will be protected under the Policy if you share information publicly and any of the following conditions are met:
- You reported the issue both internally and externally (or just externally), but no appropriate action was taken within: (i) three months after the report was submitted or (ii) within a reasonable time, not exceeding three months (or up to six months in duly justified cases for external reports) after the report was submitted, or
 - You have good reasons to believe that:
 - the issue poses an immediate or obvious danger to public interest (e.g. emergency or irreversible damage), or
 - in the case of external reporting, there is a risk of retaliation, or a low chance the issue will be effectively handled. This could be because evidence might be hidden or destroyed, or because the authority involved is not trustworthy or is connected to the problem.
- 2.4 **Retaliation according to Section 10 of the Policy:** Retaliation against a Whistleblower who in good faith raises a concern involving matters covered by the HSchG (see Section 1.2 above) is legally invalid.
- 2.5 **Processing of personal data:** In addition to the legal provisions stated in Section 13.1 of the Policy in Austria processing of personal data with regard to whistleblowing reports is governed by Section 8

of the HSchG as well as the provisions of the Austrian Data Protection Act (*Datenschutzgesetz – “DSG”*).

- **Retention period:** Personal data must be stored by CTP for five years after the report case is closed and beyond that for as long as is necessary to carry out administrative or judicial proceedings that have already been initiated or investigative proceedings under the Code of Criminal Procedure (*Strafprozessordnung – “StPO”*).
Processing operations actually carried out, such as in particular changes, queries and transmissions, must be logged. Log data on these processes must be kept three years after the five years retention obligation ceases to apply.
- **Data subject rights:** As long as and insofar as this is necessary to protect the identity of a Whistleblower or persons according to Section 10.4 of the Policy in order to achieve the purposes of the Policy, in particular to prevent attempts to prevent, undermine or delay reporting or follow-up measures based on reports, in particular for the duration of administrative or judicial proceedings or investigative proceedings under the StPO, the following rights of a natural person affected by a report shall not apply: Right to information, rectification, erasure, restriction of processing, to object and to notification of a personal data breach.

3. EXTERNAL REPORTING

3.1 As stated in Section 12 of the Policy, you are primarily encouraged to report concerns internally. Alternatively, you can also report concerns externally.

3.2 Whistleblowers should check whether they can first submit a report internally. Concerns should be reported to an external body in particular if it is not possible, not appropriate or not reasonable to handle the information in the internal whistleblower system or if it has proven to be unsuccessful or futile.

3.3 The [Federal Bureau of Anti-Corruption and Prevention of Corruption](#) (*Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung*) is the external body primarily responsible for external reports. Insofar as the following bodies or systems are responsible, in particular on the basis of the following federal laws, the Federal Bureau of Anti-Corruption and Prevention of Corruption is not responsible:

- The internet-based whistleblower system set up at the Federal Competition Authority (*Bundeswettbewerbsbehörde*) pursuant to Section 11b (6) of the Austrian Competition Act (*Wettbewerbsgesetz*)
- The Financial Market Authority (*Finanzmarktaufsichtsbehörde*) on the basis of the legal acts listed in Section 2 of the Financial Market Authority Act (*Finanzmarktaufsichtsbehördengesetz*)
- The Money Laundering Reporting Office (*Geldwäschemeldestelle*) on the basis of Section 4 (2) no. 1 and 2 of the Federal Criminal Police Office Act (*Bundeskriminalamt-Gesetz*)

3.4 Provided that the requirements of Section 8.1 of the Policy are met, Whistleblowers shall qualify for protection also in case of external reporting.



Annex BULGARIA

ANNEX – INTERNAL RULES AND PROCEDURES

for internal reporting and subsequent actions of CTP Invest EOOD under the Protection of Persons who Report or Publicly Disclose Information on Breaches Act.

1. GENERAL PROVISIONS

Article 1

Framework

- (1) These Internal Rules and Procedures (the “Rules”) of CTP Invest EOOD (the “Company”) govern the terms and conditions for internal reporting and subsequent actions of The Company in accordance with the provisions of the Protection of Persons who Report or Publicly Disclose Information on Breaches Act (“PPRPDIBA”, the “Act”) and the Group Whistleblower Policy of the CTP group companies (the “CTP Group”).
- (2) The Company, officers authorized by the Company, as well as its employees are obliged to comply with the duties and obligations set forth in the Rules, the Group Whistleblower Policy, as well as the Act and secondary Bulgarian legislation for implementation of the Act (referred together as the “Law”).

Article 2

Who can Report Breaches

You can file a report if, while performing your work or official duties or in another work context (such as current and former employees, shareholder, subcontractors, etc.), you have received information about a violation in or affecting the Company. Our whistleblowing channel is open not only to our employees, but also to all persons who have information about violations in or affecting the Company obtained in a work context.

Article 3

Designated Persons

- (1) By order of the Company’s, the Company’s employees are designated to be responsible for reviewing the received reports falling within the scope of the Act:
Ivaylo Toniev Todorov, CFO Bulgaria, ivaylo.todorov@ctp.eu, phone:
below referred to as the “Designated Persons”.
- (2) In carrying out their duties, the Designated Persons responsible for the consideration of signals:
 - a. comply with these Rules;
 - b. should not be in a conflict of interest for each specific case;
 - c. have a duty of confidentiality, privacy and impartiality.

Article 4

Provision of Information

- (1) The Designated Persons maintain on the website and on the internal (Intranet) page of CTP Group up-to-date information on the terms and conditions of reporting.
- (2) The information under para. 1 shall be placed by the Designated Persons in the office and work premises of the Company in a visible place.

Article 5

Reportable Breaches

- (1) Breaches which should be reported and fall in the scope of the Act are:
 - a. breaches of the Bulgarian legislation or acts of the European Union referred to in the Annex to the Act in the areas of: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; safety and compliance of products; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; respect for privacy and protection of personal data; security of network and information systems;
 - b. breaches affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union, and as further specified in relevant Union measures;
 - c. breaches of the rules of the internal market as referred to in Article 26, paragraph 2 of the Treaty on the Functioning of the European Union, including the rules of the European Union and the Bulgarian legislation on competition and state aid;
 - d. breaches relating to cross-border tax arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
 - e. committed criminal offence of a general nature, of which a person has become aware in connection with the performance of his/ her work or his/ her official duties.
- (2) The Rules and the Act shall also apply to reports on breaches of Bulgarian law concerning:
 - a. the rules for payment of outstanding public state and municipal receivables;
 - b. the labour law;
 - c. the legislation related to the performance of public service.
- (3) Other breaches not falling under para. 1 and 2 (for example improper use of the CTP Group's resources, violations of the policies on gifts and hospitality etc.) could be reported on global level, as per the Group Whistleblower Policy.
- (4) The Rules and the Act do not apply to consideration of complaints, reports or other requests, regardless of how they are titled, through which only the protection of personal rights is sought, or they concern interpersonal relations, without any indication of affected public interest.

Article 6

Protection of Whistleblowers and Other Persons

- (1) When you report a violation under the Act, the report is not anonymous, and at the time of the report you had reason to believe that the information in the report was true, you are guaranteed the following protections:
 - a. Confidentiality - your identity will be kept confidential and will not be disclosed to others both during and after the investigation of your report has been completed, unless absolutely necessary or with your written consent;

- b. Protection against retaliation - you will be protected from any retaliatory actions, as well as threats or attempts to do so in connection with your report. If, as a whistleblower, you become subject to such retaliation, please notify the Designated Employee so that immediate assistance can be provided;
 - c. Release of Liability for Receipt, Access and Disclosure of Information - you will not be liable for receiving or accessing the information communicated unless it constitutes a crime. You will not be liable for disclosure of information provided that you had reasonable grounds to believe that the information was true and that the reporting was necessary to detect the breach. However, please note that your actions cannot be arbitrary and the protection under the Act is not unlimited. You may be subject to disciplinary, administrative, criminal or other liability in accordance with applicable law, as well as liability for damages caused by you reporting or publicly disclosing information, if you knowingly provide or disclose false information.
- (2) Protection against retaliation under the Rules and the Act shall be granted to:
- a. a reporting person (whistleblower) from the moment of submitting the report or the public disclosure of information on a breach.
 - b. persons who assist a reporting person in the whistleblowing process and whose assistance shall be kept confidential;
 - c. persons who are connected with the reporting person or relatives of the reporting person and who could suffer retaliation as a result of the reporting;
 - d. legal entities in which the reporting person is a shareholder and for which he/she works or with whom he/she is otherwise connected in a work-related context.
- (3) Conditions for protection of reporting persons: a person reporting a breach through internal or external channels within the meaning of the Act shall have the right to protection, where the following cumulative conditions are satisfied:
- a. he/she has had reasonable grounds to believe that the information on the breach in the report was correct at the time of its submission and that this information falls within the scope of Article 3 of the Act which are listed in Article 5 of the present Rules;
 - b. he/she has reported a breach under the conditions and according to the procedure of the Act, outlined in the present Rules.

2. INTERNAL WHISTLEBLOWING PROCEDURE

Article 7

Initiation of the Procedure

- (1) A report may be submitted via the internal reporting channel of the Company, as described in the present Rules, or external reporting channel, established by the CPDP, or both.
- (2) We encourage you to submit reports through the Company's internal reporting channel so that they can be dealt with quickly and efficiently.
- (3) The procedure for consideration of reported breaches begins with the receipt in the Company of a report for a breach under the terms and conditions of the Act.

Article 8

How to Report a Breach

- (1) An internal channel is established at the Company through which a breach may be reported, either verbally or in writing. Reports for breaches shall be submitted to the Designated Persons.
- (2) Written signals shall be submitted by:

- a) e-mail to the Designated Persons [ivaylo.todorov@ctp.eu], or
 - b) through a shipment address to [Ivaylo Toniev Todorov], containing the following text under the address of the recipient: "signal under the PRRPDIBA", at the address of the Company: Bulgaria, Sofia, Saborna 2a str., fl.4. The shipment is immediately handed over to one of the Designated Persons, without being opened by the recipient; or
 - c) by using the Whistleblowing platform: more information is available on the Intranet [<https://intranet.ctp.eu/web/guest/whistleblowing-bulgaria>].
- (3) When submitting a written report, please fill out the "Form for registration of a signal for submission of information about violations" (the "Form"), according to the template approved by the Commission for Personal Data Protection (the "CPDP"), which you can download HERE [<https://cpdp.bg/%D1%84%D0%BE%D1%80%D0%BC%D1%83%D0%BB%D1%8F%D1%80-%D0%B7%D0%B0-%D1%80%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%80%D0%B8%D1%80%D0%B0%D0%BD%D0%B5-%D0%BD%D0%B0-%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB-%D0%BF%D0%BE/>]. You can also submit a written report in a free form. When submitting a free-form report, please provide your contact details so that we can contact you to clarify the information on the report, as well as to notify you of the development and actions taken on your report.
- (4) Access to the content of the e-mail is provided only to the Designated Persons.
 - (5) Oral reporting of breaches shall be submitted by telephone [insert phone number(s)] or at the request of the reporting person, through a personal meeting, within an appropriate timeframe agreed with a Designated Employee within the Company's established business hours.
 - (6) The oral report of a breach shall be documented by one of the Designated Persons by filling in the Form. The reporting person is offered and is given the opportunity to sign the Form at their discretion.
 - (7) Your report must be as complete, true, objective and unbiased as possible and contain enough specific information to permit verification. The report must contain specific data about a violation or a real danger that it will be committed, the place and period of the violation, a description of the act or the situation and other circumstances, as far as they are known. You can attach any documents or information to your report to support your statements, and you can indicate the persons who could confirm the data you reported or provide additional information.

Article 9

Forwarding Reports

- (1) In the event that a report for violations of the Bulgarian legislation in the areas referred to in Article 3 of the Act outlined in Article 5 of the Rules, or of the acts of the European Union referred to in the annex to the Act, falls to an employee other than the Designated Persons, the employee receiving it shall be prohibited from disclosing any information, which could identify the reporting or the affected person and forward the report immediately to one of the Designated Persons in the Company.
- (2) If a report is submitted which is not within the competence of the Company, it shall be immediately forwarded by one of the Designated Persons to the CPDP.

Article 10

Anonymous and Late Reports

- (1) We encourage you to report a violation as soon as possible after learning or discovering a violation so that we can act on it as quickly and efficiently as possible. Reports concerning violations committed more than two years ago are not considered, unless it is a serious violation.
- (2) As a rule and according to the Act, anonymous reports are not considered. If, however, the anonymous report contains sufficient information to permit investigation, the Company may, in its sole discretion, conduct an investigation and take follow-up action as necessary to stop or prevent the violation.

Article 11

Register of Reports

- (1) The Company shall establish and maintain a Register of reports (the "Register") under Article 18, para. 2 of the Act, according to the form approved by the CPDP. The Register is not public.
- (2) The Register shall be kept by the Designated Persons. Only the Designated Persons shall have access to the Register.
- (3) The procedure for keeping the Register shall be determined by an order of the Company.

Article 12

Document Processing and Storage

- (1) The electronic documents pertaining to reported breaches as well as the documents on reported breaches submitted on paper shall be kept by the employees under art. 2, organized in a way that ensures their confidentiality and security.
- (2) New documents concerning a reported breach already submitted shall be subject to registration under the same number.
- (3) The reports and the materials attached to them, including the subsequent documentation related to their consideration, are stored by the Company for a period of 5 years after the completion of consideration of the report, except in the presence of criminal, civil, labor law and/or administrative proceedings in connection with the submitted report.
- (4) The documents pertaining to reported breaches are subject to compliance with the Company's Privacy Policy available at <https://ctp.eu/ctp-policies/>.

Article 13

Registration Process

- (1) After receiving the report relating to breaches, the Designated Persons shall take action to generate a unique identification number (UIN) from CPDP's official website as soon as possible, without undue delay and to register the reported breach in the Register.
- (2) Within 7 days from the date of receipt of the reported breach the Designated Persons shall carry out a regularity check and its receipt shall be acknowledged by providing the reporting person with information about the UIN and the date of registration of the reported breach.
- (3) If the reported breach does not meet the requirements of art. 15, para. 2 of the Act, the reporting person shall be sent a notice for removal of the irregularities within 7 days of receipt of the reported breach.
- (4) If the irregularities on the reported breach are not removed within the term under para. 3, the Designated Employee returns the report for the breach to the reporting person, together with the attachments thereto.

Article 14

Reports Check

- (1) Each reported breach shall be checked by one of the Designated Persons in terms of its permissibility and authenticity. If the investigation reveals that the reported breach does not fall within the scope of the PRRPDIBA and its content does not give grounds to be considered plausible, the report together with the annexes thereto shall be returned to the reporting person.
- (2) Reports for breaches containing obviously false or misleading statements of facts shall be returned with an instruction to the sender for correction of the allegations and for the responsibility they bear for accusation.

Article 15

Investigation and Subsequent Actions

- (1) In the event that the report is subject to consideration, investigation shall be carried out.
- (2) In case the facts presented in the report are confirmed, the Designated Employee:
 - a. takes subsequent actions with regard to the report;
 - b. prepares an individual report containing information on the reported breach, the subsequent actions taken and proposals for taking specific measures to stop or prevent the breach;
 - c. attaches as written appendices to the report the evidence gathered in the course of the investigation.
- (3) Within a period not longer than three months after acknowledging the receipt of the reported breach, one of the Designated Persons, having examined the relevant reported breach, prepares an individual report which briefly describes the information from the report, the actions taken, the final results of the check, which, together with the reasons, shall be communicated in writing to the whistleblower and the person concerned, subject to the obligation to protect them.
- (4) When your report falls within the scope of the Act, no later than three months from the confirmation of receipt of the report, the Designated Employee will provide you with feedback on the actions taken in relation to the report you submitted. The information is provided regardless of whether the investigation has been completed or is still in progress. You may at any time request information from the Designated Employee regarding the report you submitted. After the report check is completed, you will receive information about the final results of the check.

Article 16

Documenting and Prioritizing Reports

- (1) All actions of the Designated Persons in the course of the work on the reported breach shall be documented.
- (2) The Designated Persons follow the Company's predetermined criteria and rules for prioritizing more serious breaches when handling multiple reports received.

Article 17

Protection of the Identity of the Whistleblower

- (1) Access to the information related to the reported breaches and the protection of the identity of the reporting persons shall be granted only to the employees to whom such data are necessary for the performance of their duties.
- (2) The transmission of data and the reference to circumstances may not directly or indirectly disclose the identity of the reporting person, as well as create an assumption about his/ her identity.
- (3) The documents drawn up, access to which is provided to persons in the course of exercising their duties shall not contain data or information on the reporting person or any other information from which his/ her identity can be directly or indirectly known.

Article 18

Personal Data Protection

- (1) No personal data shall be collected which are manifestly not relevant for the examination of the reported breach, and if accidentally collected, shall be deleted.
- (2) Any processing of personal data, including the exchange or transmission of personal data by competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680, and where institutions, bodies, offices or agencies of the European Union participate in the transfer – in accordance with Regulation (EU) 2018/1725, as well as with the Personal Data Protection Act.

3. FINAL PROVISIONS

Article 19

Applicable Provisions

- (1) For the outstanding issues in these Rules, the relevant provisions of PPRPDIBA shall apply.
- (2) The present Rules supplement the Group Whistleblower Policy of CTP Group, addressing local specifics in Bulgaria. Where there is a difference, the Rules will take priority over the Group Whistleblower Policy to ensure full compliance with the Law.

Article 20

Adoption and Revision of the Rules

- (1) The Rules are approved by an Order of the head of the Company and enter into force from the date of their approval.
- (2) Amendments and additions to the Rules are carried out in the order of their adoption.
- (3) A review of the Rules is carried out at least once every three years, analyzing the practice of their application and updating them if necessary.

Article 21

Communication with the CPDP

The Designated Persons are obliged to regularly submit the necessary statistical information under the Act to the CPDP according to the procedure established by it, including information on the number of reports received and the number of inspections performed and their results.

Article 22

Enforcement Measures

- (1) All employees of the Company and persons who have contact with the Company in a work context should familiarize themselves with the Rules.
- (2) Any violation of the Rules is grounds for seeking disciplinary liability, according to the provisions of the Labor Code, as well as any other type of liability, according to Bulgarian legislation.

Article 23

Where to Find More information

For questions related to whistleblowing and whistleblower protection, please contact the Designated Persons at the contact details specified in Article 3 above.



Annex CZECH REPUBLIC

1 INTRODUCTION

- 1.1 This annex **governs deviations from the Policy regarding local (Czech) whistleblowing channel** established for the company CTP Invest, spol. s r.o., identification number: 26166453, with its registered office located at CTPark Humpolec 1571, 396 01 Humpolec, registered with the Regional Court in České Budějovice, file number: C 15647 (the "**Company**"). Matters not explicitly regulated in this annex shall be governed by the main Policy.
- 1.2 Main legal basis with regard to whistleblowing in Czechia is the Act No. 171/2023 Coll., on the Protection of Whistleblowers (the "**Czech Whistleblower Protection Act**") and Act No. 253/2008 Coll., on Certain Measures against Money Laundering and Terrorist Financing (the "**Czech AML Act**").

2 WHO CAN REPORT?

- 2.1 Any employee and individual, including third parties, who is engaged with the Company otherwise than in a basic labor-law relationship, including any individual who has performed or is performing work or other similar activity* for the Company, even indirectly, or has been or is in contact with the Company in connection with such activity or is applying for such activity may submit a report via local (Czech) whistleblowing channel.

***Work or other similar activity** means:

- dependent work performed under an employment relationship;
- self-employment;
- exercise of rights associated with participation in the Company;
- performance of the function of a member of the Company's body;
- fulfilment of tasks within the activities of the Company, in its interest, on its behalf, or at its expense;
- administration of a trust fund;
- voluntary work;
- professional practice, internship;
- exercise of rights and obligations arising from a contract whose subject is the provision of supplies, services, construction works, or other similar performance.

An individual who makes a report via local (Czech) whistleblowing channel or who publicly discloses⁵ information on Breaches is called whistleblower (the "**Whistleblower**").

3 WHICH CONCERNS ARE COVERED BY THIS POLICY (INCLUDING THIS ANNEX)?

3.1 Any conduct which has already occurred or may occur involving the Company that represents or may represent Breaches or any attempts to conceal the Breaches may be reported via the local whistleblowing channel. This includes all the concerns listed in Article 3 of the Policy.

Below, see the **additional examples** of Breaches that should be reported:

- conduct that has the characteristics of **any criminal offence** (e.g. fraud, theft, bribery, embezzlement);
- conduct that has the characteristics of a more serious **administrative offence**, which is punishable by a fine of CZK 100,000 or more (e.g. violations of labour law, such as discrimination of employees, failure to provide wages by the due date);
- **violation of other legal regulations or European regulations in the area of:** financial services, due diligence and other assurance services, financial products and financial markets, corporate income tax, prevention of money laundering and terrorist financing, consumer protection, compliance with product requirements, including product safety, transport and road safety, protection of the environment, food and feed safety and animal health, radiation protection and nuclear safety, competition, public auctions and public procurement, protection of internal order and security, life and health, protection of personal data, privacy and security of electronic communications networks and information systems, protection of the financial interests of the European Union, or the functioning of the internal market, including the protection of competition and state aid under European Union law;
- **violation of the Czech Whistleblower Protection Act.**

In-person Meetings According to Section 4. 2 of the Policy

3.2 In case you want to make a report by means of an in-person meeting with the Designated Person, such meeting shall take place within the reasonable timeframe after the request is made, but **no later than 14 days from the date the request was made.**

4 WHO AND HOW SHOULD I REPORT TO?

Reporting on the Local Level

4.1 The provisions of Article 4 of the Global Whistleblower Policy remain in effect. For your convenience, we provide references to reporting options at the local level:

4.2 The whistleblowing channels enable reporting **in writing or orally via hot line**. Upon your request, the report can be made also by means of a **in-person meeting with the Designated Person**, which shall take place within the reasonable timeframe after the request is made.

⁵ 'Public disclosure' or 'to publicly disclose' means the making of information on Breaches available in the public domain. For more information see Section 7.4 to this annex.

4.3 When reporting through the local whistleblowing channel, you have the following options:

- **Whistleblowing platform:** more information is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing-czech-republic>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).
- **Post mail:** postal item to be sent to the address of the respective CTP Group entity, to the attention of the respective Designated Person (**do not forget to include the name of the Designated Person on the envelope!**)
- **Hot line:** the phone number for the hotline for individual CTP Group entities is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing-czech-republic>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).
- **In-person meeting:** please, contact the Designated Person for your CTP Group entity.
- **E-mail to the Designated Persons:** use the email address specifically designated for receiving whistleblowing reports, available on the intranet ((<https://intranet.ctp.eu/web/guest/whistleblowing-czech-republic>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>)).

Recording of the Oral Report (additional provision)

In addition to the Global Whistleblower Policy, here is the procedure for submitting a report verbally:

- 4.4 In the case of receiving a report via a telephone line or in a face-to-face meeting, provided that there is consent given by the Whistleblower, an audio recording of the oral report can be made.
- 4.5 If no audio recording has been made, the Designated Person shall make a written record of the report which faithfully captures the substance of the oral report.
- 4.6 The Designated Person shall give the Whistleblower an opportunity to comment on the written record of the report or transcript of the audio recording. The Whistleblower's comments shall be attached to the recording or transcript.

5 CAN I REMAIN ANONYMOUS?

- 5.1 The Company encourages an open culture and emphasizes the importance of raising any concerns openly to assess, investigate and gather additional information, if needed.
- 5.2 If the Whistleblower raises concerns openly, the Company will use all reasonable efforts to ensure the Whistleblower's identity will not be revealed without the Whistleblower's previous written consent (unless the Company required to comply with the Legislation) and treat the report confidentially according to the rules set in Article 5 of this annex. However, if you do not wish to openly raise concerns, you can report anonymously.
- 5.3 **Anonymous reports submitted via the local whistleblowing channel will be treated, to the extent permitted by the nature of the matter, in the same manner as the reports from which the identity of the Whistleblower can be inferred.** Whistleblowers who make anonymous reports will be provided

with the same protection, to the extent permitted by the nature of the matter, as the Whistleblowers who disclose their identity.

- 5.4 The Whistleblowers who reported via local whistleblowing channel or Publicly Disclosed information on Breaches anonymously, but who are subsequently identified, shall be protected provided that they meet the conditions laid down in Article 7 of this annex.

6 WHAT HAPPENS AFTER I REPORT A CONCERN?

- 6.1 The provisions of Article 7 of the Global Whistleblower Policy remain in effect. Article 7.5. of the Global Whistleblower Policy is amended to read as follows:

The Designated Person will assess the merits of the report and notify the Whistleblower in writing of the assessment results within **30 days from the date of receiving the report**. In cases that are factually or legally complex, this deadline may be **extended by up to 30 days, but no more than twice**. The Designated Person will inform the Whistleblower in writing about the extension and the reasons for it before the original deadline expires. In the case of an anonymous report, the Whistleblower will be notified according to this article if the Whistleblower provides appropriate contact information they wish to be notified on.

7 WHO IS PROTECTED UNDER THIS ANNEX?

- 7.1 The protection under this annex applies to the Whistleblowers who have made a report regarding matters covered by the Policy including this annex:
- via the local whistleblowing system; or
 - via the external whistleblowing system; or
 - by making a public disclosure (see Section 7.4) of the report.
- 7.2 The protection against retaliatory measures under this annex also applies to a person who has made a report to a public authority competent under another legal regulation than the Whistleblower Protection Act or directly applicable regulation of the European Union.
- 7.3 The protection against retaliatory measures does not apply to a person who has made a report without having had reasonable grounds to believe that the information in the report was true.

Public disclosure

- 7.4 Public disclosure means that the Whistleblower:
- has made a report through the local (Czech) whistleblowing system and the external reporting system (see Article 9 of this annex), or only the external reporting system, and appropriate action has not been taken within the time limits set out in the Czech Whistleblower Protection Act, in particular, the Designated Person has not assessed the reasonableness of the report under section 12(3) of the Czech Whistleblower Protection Act, the Company has not taken other appropriate action to prevent or remedy the unlawful condition under the section 12(5) of the

Czech Whistleblower Protection Act, or a civil servant under section 13 of the Czech Whistleblower Protection Act has not assessed the report under the section 17(1) of the Czech Whistleblower Protection Act; or

- has reasonable grounds to believe that the infringement referred to in the report may lead to an imminent or obvious threat to internal order or security, life or health, the environment or other public interest or to irreparable harm; or
- has reasonable grounds to believe that, if the report is made through the external reporting system, there is an increased risk, given the circumstances of the case, that they or a person described in section 4(2)(a) through (h) of the Czech Whistleblower Protection Act will be subject to retaliation or that the Title III process of the Czech Whistleblower Protection Act is at risk.

7.5 The protection under this annex applies also to other protected persons, who are related to the Whistleblower or the report, specifically:

- a) a person who has provided assistance in ascertaining the information contained in the report, filing the report or assessing its reasonableness;
- b) a person who is a close person to the Whistleblower;
- c) a person who is an employee or colleague of the Whistleblower;
- d) a person controlled by the Whistleblower;
- e) a legal entity in which the Whistleblower has an interest, a person controlling it, a person controlled by it or a person who is controlled by the same controlling person as the legal entity;
- f) a legal entity of which the whistleblower is a member of an elected body, a controlling person, a controlled person, or a person controlled by the same controlling person;
- g) a person for whom the whistleblower performs work or other similar activity within the meaning of the Act;
- h) a trust of which the whistleblower or a legal entity referred to in point (e) or (f) is a settlor or a defendant or in relation to which the whistleblower or a legal person referred to in point (e) or (f) is a person who substantially increases the assets of the trust by contract or by acquisition on death.

("Other Protected Persons")

8 HOW MY IDENTITY WILL BE PROTECTED AND WILL THE REPORTS BE TREATED CONFIDENTIALLY?

8.1 Only the Designated Persons for the Czechia have access to the reports submitted through the local whistleblowing system.

8.2 Designated Persons shall treat all the reports confidentially to enable adequate investigation and to comply with applicable data protection legislation and requirements of the Czech Whistleblower Act and the Czech AML Act and other Legislation. They maintain confidentiality about the facts

they learned during the performance of their activities even after the termination of the performance of these activities, unless otherwise provided by the law.

8.3 Designated Persons shall not provide information that could frustrate or jeopardise the purpose of making reports.

Protection of the identity of the Whistleblower and Other Protected Persons

8.4 In all cases, information regarding the **identity of the Whistleblower and Other Protected Persons** may only be disclosed with their prior written consent, unless the Designated Person is obligated to provide such information to the competent authorities under legal regulations. . This shall also apply to any other information from which the identity of the Whistleblower or Other Protected Persons may be directly or indirectly deduced (e.g. work position, birth date etc.).

8.5 If the Designated Person discloses information regarding the identity of the Whistleblower to a public authority in accordance with the previous sentence, they are obliged to inform the Whistleblower in advance, together with the reasons for which they are obliged to provide the information, and allow the Whistleblower to express their views on the disclosure of the information

8.6 The exercise by the respondents of their right to access by virtue of the Data Protection legislation shall not involve access to the identity of the Whistleblower or Other Protected Persons

Other confidential information

8.7 If **all** the above conditions are met, the Designated Person may disclose partial (necessary) information regarding the report in order to properly investigate the report or to enable corrective action to be taken (e.g. to its own Compliance personnel involving auditors and Compliance personnel from other parts of the CTP Group), and/or involve professional advisors from outside the Company. Such persons are obliged to observe the same level of confidentiality.

Notification of a person concerned

8.8 The Company will generally notify the person implicated in a report that concerns have been raised in relation to him or her unless it could jeopardize the proper follow-up or there were other justifiable reasons for it. The Company will make this notification within a reasonable time and take into consideration the interests of the investigation. The Company will take all reasonable measures to prevent the person implicated in a report from learning the identity of the Whistleblower or Other Protected Persons.

9 THE EXTERNAL REPORTING SYSTEM

9.1 You have the right to report to the Ministry of Justice of the Czech Republic. Information about reporting to the Ministry of Justice of the Czech Republic is set out on the website: <https://oznamovatel.justice.cz/> .

Although we recognize that in some circumstances it may feel appropriate for you to raise your concerns to an external body, we encourage you to report via the designated internal channels before reporting to anyone outside of the CTP Group.

Annex GERMANY



1 INTRODUCTION

1.1 In Germany, the protection of Whistleblowers is regulated in the Law on the Protection of Whistleblowers “Gesetz zum Schutz von hinweisgebenden Personen”, also called “Hinweiserschutzgesetz” or in short: “HinSchG”.

1.2 In addition to the rules set out in this Policy, the following rules need to be considered:

2 WHICH TYPE OF BREACHES ARE COVERED BY THE HINSCHG?

2.1 German law protects Whistleblowers who report on

- Breaches of Legislation that are punishable by (criminal) law,
- Breaches of Legislation that are subject to a fine if the violated regulation serves to protect life, limb or health or to protect the rights of employees or their representative bodies,
- Breaches of EU acts as well as its local German equivalents and implementations in the areas set out in paragraph 3.3 above
- Breaches of Legislation on public procurement
- Breaches of Legislation for financial institutions
- Breaches of tax Legislation
- Statements of public servants (“Beamte”) constituting a breach of the duty of loyalty to the constitution

2.2 Notwithstanding this list of potential topics of a report and paragraph 1.5 of the Policy, CTP Group grants further and broader protection of the Whistleblower in accordance with paragraphs 3.4 and 8 of this Policy.

3 HOW CAN I MAKE A REPORT?

3.1 Under the German HinSchG, you have a choice whether you want to make an internal report (described in Article 4) or an external report (described in Article 12). However, preferably under the Law, you should first try and make an internal report. As set out in paragraph 6 of the Policy, the report can also be anonymous.

3.2 For local matters to be reported, please use the local internal Whistleblower platform described in paragraph 4.3 of the Policy.

3.3 If internally you cannot obtain the support you find necessary, you can make a report to the following external authorities:

- Externe Meldestelle des Bundes beim Bundesamt für Justiz
[BfJ - Hinweisgeberstelle \(bundesjustizamt.de\)](https://www.bundesjustizamt.de)
- Bundesanstalt für Finanzdienstleistungsaufsicht – for reports relating to financial services and banks
- Bundeskartellamt – for breaches relating to competition law and the Digital Markets Act
[Bundeskartellamt - Hinweise auf Verstöße](#)

4 WHICH REPORTS MAY TAKE PRECEDENCE OVER THE REPORTS UNDER THIS POLICY AND THE HINSCHG?

4.1 The following rules take precedence over the reports protected under the HinSchG.

- paragraph 6, subparagraph 5 and paragraph 53 of the German Money Laundering Act
- paragraph 25a (1) sentence 6 no. 3 of the German Banking Act and paragraph 13 (1) of the German Securities Institutions Act,
- paragraph 58 of the Securities Trading Act,
- paragraph 23 (6) of the Insurance Supervision Act,
- paragraph 28 (1) sentence 2 no. 9 and paragraph 68 (4) sentence 3 of the Capital Investment Code,
- paragraph 3b and 5 (8) of the Stock Exchange Act,
- paragraph 55b (2) no. 7 of the Auditors' Code,

5 PROTECTION OF THE IDENTITY OF THE WHISTLEBLOWER

5.1 According to paragraph 9, subparagraph 1 HinSchG and in addition to paragraph 9.2 of this Policy, the identity of the whistleblower is not protected if he or she intentionally or through gross negligence reports incorrect information on Breaches.

Annex HUNGARY



ANNEX In compliance with the Act XXV of 2023 on complaints, notifications of public interest and rules on whistleblowing, hereinafter: “W Act”.

The Company, in compliance with its obligations pursuant to the relevant applicable laws of the European Union furthermore to ensure the necessary measures to protect whistleblowers as much as possible, adjusts and updates the provisions of present Policy with the present Annex in accordance with the applicable Hungarian laws as set out below.

- I. The Company is entitled to apply a uniformed whistleblower reporting system, hereinafter: system, provided that it complies with the “W Act”, and thus, subject to the obligation to set up a whistleblower reporting system pursuant to Article 18(1) of the “W Act”, declares that it will apply the system regulated in present Policy for the companies of the group that are registered in Hungary.

Once any notification has been made, the competent person shall send an acknowledgement within seven days in accordance with Article 22 (1) of “W Act” and shall investigate the matter within the shortest time possible in accordance with the circumstances, but not later than thirty days from the date of receipt of the notification, in accordance with Article 22 (2) of “W Act”.

The applicable time limit may be extended solely in particularly justified cases, provided that the whistleblower is informed accordingly simultaneously. In such case, the whistleblower shall be informed of the expected final date of the investigation and the reasons for the extension.

The investigation of the notification may be omitted if

- (a) the notification was made by an unidentified/anonymous notifier,
- (b) the notification was not made by the person entitled to do so,
- (c) a repeated notification was submitted by the same whistleblower with the same content as a previous notification; or
- (d) the harm to the public interest or to an overriding private interest would not be proportionate to the restriction of the rights of the natural or legal person (hereinafter

together referred to as the "person concerned") resulting from the investigation of the notification.

- II. The operator of the internal reporting system shall inform the whistleblower in writing regarding the investigation or non-investigation of the report and the reasons for any non-investigation, the outcome of the investigation, and if any action had been taken or planned to be taken.

The written information may be omitted if the whistleblower has been informed orally by the operator of the system of the process and has accepted and taken note of this certain presentation of the information.

- III. The operator of the system, hereby provides clear and easily accessible information in present policy on the operations of the internal whistleblowing system, the process, the systems and procedures that are applicable under "W Act".

Within the framework of the internal whistleblower reporting system

- a) the whistleblower's;
- b) the person's whose action or omission induced the notification, and;
- c) to any person's, who may have information relevant to the subject matter of the notification, personal data that is essential for the investigation of the notification may be processed solely for the purpose of investigating the notification and remedying or ceasing the action that is the subject of the notification and may be transferred to a lawyer assisting with the investigation of the notification or any external body involved in the investigation of the notification.

Any personal data that is not deemed to be in accordance with the above stated provisions and processed in the system should be deleted without any delay from the system.



Annex THE NETHERLANDS

STATUTORY DEVIATIONS TO THE CTP GROUP WHISTLEBLOWER POLICY IN ACCORDANCE WITH DUTCH LAW

1 LOCAL LEGISLATION

1.1 As a result of the adoption of the EU Directive on the Protection of Whistleblowers, the Dutch Whistleblowers Protection Act (“**WPA**”) (please find the weblink [here](#)) has partly entered into force on 18 February 2023. The sections of the WPA with respect to anonymous reporting and enforcement by the relevant authority, the House of Whistleblowers, will enter into force at a later date.

2 MATERIAL SCOPE OF A BREACH

2.1 The WPA contains a regulatory framework on the basis of which alleged misconduct can be reported both internally as well as externally (hereinafter referred to as a: “**Breach**”).

2.2 A Breach as per the WPA is:

- (i) A breach or risk of breach of Union law, related to the following areas:
- public procurement;
 - financial services, products and markets and prevention of money laundering and terrorist financing;
 - product safety and conformity;
 - transport safety;
 - environmental protection;
 - radiation protection and nuclear safety;
 - food and feed safety, animal health and welfare;
 - public health;
 - consumer protection;
 - protection of privacy and personal data, and security of networks and information systems.

The following breaches are also concerned:

- any breach affecting the financial interests of the European Union; *and*
- any breach relating to the internal markets, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements with the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

- (ii) an act or omission whereby the public interest is at stake, such as:
- a breach or a risk of breach of statutory provisions and certain internal provisions;
 - risks related to public health;
 - risks related to the safety of persons;
 - environmental risks;
 - risks related to the functioning of the public service;
 - risks related to the business due to negligent acts or omissions.

3 EXTERNAL REPORTING

3.1 The following authorities are considered competent authorities by the WPA to receive and process reported Breaches:

- Authority for Consumer and Markets
- Authority for the Financial Markets
- Data Protection Authority
- Nederlandsche Bank N.V.
- Whistleblowers Authority (*Huis voor klokkenluiders*)
- Health and Youth Care Inspectorate
- Dutch Healthcare Authority
- Authority for Nuclear Safety and Radiation Protection

4 LOCAL DEVIATIONS TO THE POLICY

4.1 *Introduction*

Article 1 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

4.2 *Who can report?*

Article 2 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

4.3 *Which concerns are covered by this Policy?*

Article 3 of the Policy applies for the Netherlands as well, with the addition that the definition of a (risk of a) breach (i.e. a Breach) is further defined and explained in Article 2 of this Annex.

4.4 *Who and how should I report to?*

Article 4 of the Policy applies for the Netherlands as well, with the understanding that a Whistleblower can submit a report related to a Breach (as defined in Article 2 of this Annex) via the channels included in the Policy in the following manners:

- In writing;
- Orally (for example by telephone conversation or voice message);
- During a meeting at a specific location (within a reasonable time at the request of the Whistleblower).

The Whistleblower has the right to file a report directly with the external reporting channels of the competent authorities as referred to in Article 3 of this Annex. It should be noted that, in line with the EU Directive on the Protection of Whistleblowers, the Whistleblower is urged to first file a report internally.

4.5 *What should the report contain?*

Article 5 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

4.6 *Can I remain anonymous?*

The sections of the WPA with respect to anonymous reporting and enforcement by the relevant authority, the House of Whistleblowers, will enter into force at a later date and therefore this Article is subject to changes in Dutch legislation.

4.7 *What happens after I report a concern?*

Article 7 of the Policy applies for the Netherlands as well, with the addition that according to the WPA, the Dutch entity(-ies) of the CTP Group will also keep a register containing information on reported Breaches. The data with respect to these registered Breaches will be destroyed if such data is no longer required to adhere to the requirements of the WPA or the requirements of other (Union) laws.

4.8 *Who is protected under this Policy?*

Article 8 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

4.9 *How my identity will be protected and will the reports be treated confidentially?*

Article 9 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

4.10 *How will I be protected against retaliation if I report a concern?*

Article 10 of the Policy applies for the Netherlands as well, whereby the WPA explicitly mentions the following examples of retaliation, which includes threats of retaliation and attempts of retaliation, which does not constitute a limited overview:

- Dismissal or suspension
- A fine within the meaning of Article 7:650 of the Dutch Civil Code
- Demotion
- Withholding a promotion
- A negative performance review
- A written reprimand
- Transfer to another branch office of the employer
- Discrimination
- Intimidation, bullying or exclusion
- Libel (*smaad*) or slander (*laster*)
- Prematurely terminating an agreement for the provisions of goods or services; and
- Revocation of a permit

In addition, it should be noted that Whistleblowers are not liable when reporting or disclosing a Breach in accordance with this Policy for violating restrictions related to the disclosure of information, unless laws with respect to national security, the professional duty of confidentiality of lawyers, medical confidentiality, confidentiality of judicial decision-making and criminal procedure dictate otherwise. The following conditions apply: (I) there should be reasonable grounds to conclude that the reporting or disclosure of information was necessary for the disclosure of the Breach and (II) the report or disclosure was conducted in accordance with the conditions as laid-down in the WPA.

4.11 *Can I ask someone for advice?*

Article 11 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

4.12 *Can I report concerns outside the CTP Group?*

Article 12 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

4.13 *Processing of personal data*

Article 13 of the Policy applies for the Netherlands as well, unless indicated otherwise in this Annex.

Annex ROMANIA



1 INTRODUCTION

- 1.1 This Country Addendum describes the limitations for implementing and operating the Group Whistleblower Policy in **Romania** and provides additional guidance describing the manner of receiving and handling whistleblowing reports by different reporting channels regulated by Law no. 361/2022 regarding the protection of whistleblowers in the public interest.
- 1.2 This Country Addendum is to be completed with the provisions of the Group Whistleblower Policy.
- 1.3 To the extent that there is a contradiction between the content of this Country Addendum and the content of the Group Whistleblower Policy, the provisions of this Country Addendum shall prevail.

2 WHO AND HOW SHOULD I REPORT TO?

Internal reporting

- 2.1 The Company established whistleblowing channels and appointed Ms. Eleonora Amariutei, CFO Romania as a Designated Person responsible with receiving, recording, examining, taking subsequent actions and solving reports ("**Designated Person**"). The Designated Person acts impartially and independently.
- 2.2 When reporting through the internal whistleblowing channels, you have the following options:
- **Whistleblowing platform:** more information is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing-romania>) and website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).
 - **Post mail:** postal item to be sent to the attention of the Designated Person, to the following address: Romania, Dragomiresti-Deal village, Dragomiresti Vale commune, 1 Gabriela St., Building B, groundfloor, Ilfov county (**do not forget to include the name of the Designated Person on the envelope!**)
 - **Hot line:** by calling the following **phone number: [...]**.
 - **In-person meeting:** please, contact the Designated Person.
 - **E-mail to the Designated Persons:** to the following email address: eleonora.amariutei@ctp.eu.

- 2.3 If the report refers to a violation of the law committed by the Designated Person, the report will be made directly to the company's administrator, by using any of the following channels:
- **Post mail:** postal item to be sent to the attention of the Country Head, to the following address: Romania, Dragomiresti-Deal village, Dragomiresti Vale commune, 1 Gabriela St., Building B, groundfloor, Ilfov county (**do not forget to include the name of the administrator!**)
 - **Phone:** by calling the following phone number: +421 905 519 339.
 - **In-person meeting:** please, contact the company's administrator.
 - **E-mail to the administrator:** to the following email address: peter.ceresnik@ctp.eu.
- 2.4 If, by mistake, the report reaches other person than the Designated Person, and the report does not concern breaches of the law committed by the later, the person receiving the report has the obligation to redirect the report immediately to the Designated Person and to maintain confidentiality just like the Designated Person, having the same confidentiality obligations as the latter. If the report concerns violations of the law committed by the Designated Person, the person who receives the report by mistake shall immediately transmit it to the company's administrator under confidential conditions.

External reporting

- 2.5 In exceptional cases, the whistleblower may choose to report breaches of the law by using external reporting channels, made available by public authorities, such as the reporting platform made available by the National Integrity Agency available at <https://integritate.eu/>.
- 2.6 When choosing the external reporting channel, the whistleblower can take into account aspects such as:
- a) the existence of the risk of retaliation, in case of reporting through internal channels; or
 - b) the inability to effectively remedy the breach through internal reporting channels.

3 WHAT SHOULD THE REPORT CONTAIN?

- 3.1 The report includes the following **optional elements**:
- the name and surname of the whistleblower;
 - contact details of the whistleblower;
 - the whistleblower's signature.
- 3.2 The report includes the following **mandatory elements**:
- the professional context in which the information was obtained;
 - the person(s) concerned, if known;
 - the description of the act likely to constitute a violation of the law;
 - where applicable, the evidence in support of the report; and
 - the date.

3.3 If the report does not contain the mandatory elements mentioned above, the Designated Person requests its completion, giving the whistleblower a period of 15 days to complete the report with the missing information.

4 CAN I REMAIN ANONYMOUS?

4.1 The report can be made both **anonymously** and with the **disclosure of the identity of the whistleblower**, at the latter's choice.

4.2 Anonymous reports will be dealt with in all cases, insofar as they contain indications of violations of the law. If the report is submitted anonymously and does not contain sufficient information regarding violations of the law, and if it is possible, the Designated Person requests the whistleblower to complete the report, giving a period of 15 days in which to complete the report.

5 WHAT HAPPENS AFTER I REPORT A CONCERN?

Receiving internal reports

5.1 The receipt of reports is made by the Designated Person, regardless of the internal reporting channel chosen by the whistleblower. In all cases, the Designated Person has the obligation to send to the whistleblower in the public interest the confirmation of receipt of the report, within no more than 7 calendar days from its receipt.

5.2 If the whistleblower chooses to make the report by telephone, the Designated Person has the obligation to document the report in one of the following ways:

- by making a recording of the conversation in a durable and accessible form, if at the beginning of the recording the whistleblower gives his consent;
- by a complete and accurate transcription of the conversation into a minutes.

5.3 If for technical reasons the conversations cannot be recorded, the Designated Person has the obligation to draw up a complete and accurate transcript of the conversation.

5.4 The Designated Person gives the whistleblower the opportunity to verify, rectify and agree to the content of the minutes of the conversation by signing it.

5.5 If the whistleblower requests to report in the presence of the Designated Person, the latter is obliged to draw up a minute of the conversation, in a durable and accessible form, subject to the consent of the whistleblower. The designated person gives the whistleblower the opportunity to verify, rectify and agree to the minutes of the conversation by signing it.

5.6 If the whistleblower does not consent to the transcription or recording of the conversation, the Designated Person advises the whistleblower to report in writing, using the other existing internal reporting channels.

- 5.7 If the whistleblower refuses to sign the report, the Designated Person shall mention this in the report and, where appropriate, continue the subsequent actions in accordance with this procedure.
- 5.8 If the whistleblower submits multiple reports concerning the same violation of the law, the reports are merged and treated as one report.

Registration of the reports

- 5.9 The registration of reports is made by the Designated Person who has the obligation to enter the following information in the **Register of reports** organized at the level of the Company:
- Date of receiving the report;
 - If known, the name, surname and contact details of the whistleblower;
 - Subject matter of the report; and
 - The manner of solving the report.
- 5.10 The Register of reports is drawn up in confidential conditions in electronic format by the care of the Designated Person and keeps a record of all the reports received by the company. Based on the information entered in the register, the Designated Person draws up annual statistics regarding the reports concerning violations of the law, that are presented to the company's management.
- 5.11 The reports received are archived in confidential conditions by the Designated Person for a period of 5 years, at the end of which they are destroyed, regardless of the medium on which they are kept.

Carrying out subsequent actions

- 5.12 After receiving the report and examining it, the Designated Person has the obligation to diligently carry out the subsequent actions necessary to confirm or invalidate the aspects described in the report, under conditions of confidentiality.
- 5.13 In order to carry out the subsequent actions, the Designated Person benefits from all the necessary resources to investigate the facts mentioned in the report and is entitled to take the following actions:
- To request additional information from the whistleblower regarding the facts mentioned in the report.
 - To request information and documents from the person(s) concerned in relation to the facts mentioned in the report, without revealing the identity of the whistleblower.
 - To collect all the means of evidence necessary to perform the subsequent actions, in compliance with the relevant legal provisions, especially the protection of personal data and the observance of the secrecy of correspondence.
 - Require employees/collaborators irrespective if they are or not mentioned the report to provide documents and information necessary to perform the subsequent actions, without disclosing the identity of the whistleblower or the person(s) concerned.
- 5.14 In order to carry out all the necessary diligences related to the subsequent actions, in absolutely necessary cases, the Designated Person may request the support of other employees/collaborators. In this case, the confidentiality obligations are extended to these employees/collaborators, and the

Designated Person will limit the information communicated to them to the minimum necessary to provide the requested support. The Designated Person has the obligation to remind the employees/collaborators involved in the subsequent actions the confidentiality obligations they must comply with.

5.15 Throughout the subsequent actions, the person(s) concerned have the right to defense, including the right to be heard and the right of access to their own file.

5.16 The Designated Person has the obligation to inform the whistleblower about the status of the subsequent actions within 3 months from the date of acknowledgement of receipt, as well as, subsequently, whenever there are developments in the performance of the subsequent actions, unless the information could jeopardize the development of the subsequent actions.

The outcome of the subsequent actions

5.17 After diligently performing the subsequent actions, the Designated Person may:

1. Decide the **termination of the procedure**

The termination of the procedure may be decided by the Designated Person when:

- a) As result of the subsequent actions, the Designated Person concludes that the facts described in the report are not real or do not represent violations of the law.
- b) The report does not contain the mandatory elements, and the Designated Person requested the completion of the report within 15 days, without this obligation being fulfilled.
- c) The report is submitted anonymously and does not contain enough information regarding violations of the law, which would allow the analysis and performance of the subsequent actions, and the Designated Person requested the completion of the report within 15 days, without this obligation being fulfilled.
- d) The whistleblower makes a new report on the same violation of the law, without presenting additional information that justifies a different subsequent action.
- e) Upon examination of the report, it is found that it is a clearly minor infringement and does not require further subsequent action other than the termination of the procedure.

In all cases, the termination of the procedure shall be communicated to the whistleblower, indicating the legal basis.

2. Draft a **report with proposals for the management** of the company

If the facts described in the report are confirmed and represent violations of the law, the Designated Person draws up a report with the proposal to start the disciplinary investigation or, as the case may be, with the proposal to notify the competent authorities, which he submits to the company's management.

- 5.18** The Designated Person informs the whistleblower in the public interest about the outcome of the subsequent actions.
- 5.19** In all cases, regardless of the outcome, the Designated Person informs the company's management and makes the necessary entries in the Register of reports.
- 5.20** If the person concerned is the Designated Person, all the duties and obligations of the Designated Person under this procedure shall be taken over by the company's administrator.

6 CONFIDENTIALITY OBLIGATIONS

- 6.1** Both the Designated Person and any other employees/collaborators involved in the process of carrying out the subsequent actions have the obligation not to reveal the identity of the whistleblower or of any third party mentioned in the report or any information that would allow their direct or indirect identification, unless the whistleblower expresses his consent for disclosure of his identity in a documented form.
- 6.2** Also, the identity of the whistleblower may be disclosed if this is an obligation imposed by law, in compliance with the conditions and limits provided by such law. In this case, the whistleblower shall be informed in advance in writing of the disclosure of his identity and the reasons for the disclosure of the confidential data in question. The obligation to inform the whistleblower does not exist if the information would jeopardize investigations or judicial proceedings.
- 6.3** The obligation of confidentiality is also maintained if the report is mistakenly sent to another person within the Company, other than the Designated Person. In this case, the report is immediately forwarded to the Designated Person or to the company's administrator, as the case may be.
- 6.4** The provisions of this procedure on the protection of the identity of whistleblowers also apply to the person(s) concerned, as well as to the third parties referred to in the report.
- 6.5** The identity of the person(s) concerned is protected while the subsequent actions are in progress, unless, as a result of the subsequent actions, it is found that the person(s) concerned is not guilty of the violations of the law that were the subject of the report or public disclosure. If the person(s) concerned is innocent, the obligation to protect his or her identity extends for an unlimited period.
- 6.6** The provisions of this section shall not apply if the whistleblower has intentionally disclosed his or her identity in the context of a public disclosure.

7 WHO IS PROTECTED UNDER THIS POLICY?

- 7.1** The whistleblower who internally or externally reports violations of the law or makes a public disclosure benefits of protection against any form of retaliation or attempt of retaliation in the conditions set forth by the Group Whistleblower Policy, this Country Addendum and Law no. 361/2022.

- 7.2** In addition to the provisions of Clause 8 of the Group Whistleblower Policy, the whistleblower who reports information on violations of the law does not breach the legal provisions or the contractual clauses on the disclosure of information and is not liable for the external reporting to authorities or public disclosure of such information, provided that he made an external report or public disclosure under the conditions of Law no. 361/2022 and has reasonable grounds to believe that the external reporting or the public disclosure was necessary for the exposure of a violation of the law.
- 7.3** The public disclosure can be done by providing information to the media, NGO's, professional organizations, syndicate organizations, parliamentary commissions, or by providing in any way in the public area information regarding violations of the law and entitles the whistleblower to protection in the conditions set forth by Law no. 361/2022.



Annex SERBIA

There have been no changes to Serbian whistleblowing regulations since 2014. Consequently, the Serbian-specific whistleblowing policy remains unchanged. However, updates have been made to the Group Whistleblowing Policy to reflect broader developments.



SRB
2021
100001179-0000-0629-BBC3-800524847D74

U skladu sa članom 16 Zakona o zaštiti uzbunjivača („Službeni glasnik RS“ br. 128/2014, u daljem tekstu: „**Zakon**“) i Pravilnikom o načinu unutrašnjeg uzbunjivanja, načinu određivanja ovlašćenog lica kod poslodavca, kao i drugim pitanjima od značaja za unutrašnje uzbunjivanje kod poslodavca koji ima više od deset zaposlenih („Službeni glasnik RS“ br. 49/2015 i 44/2018 u daljem tekstu: „**Pravilnik**“), privredno društvo CTP Invest doo Beograd – Novi Beograd, sa registrovanim sedištem na adresi Bulevar Zorana Đinđića broj 64a, matični broj 21287172, PIB110027463, čiji je zakonski zastupnik direktor Richard Wilkinson (u daljem tekstu: „**Poslodavac**“) dana 7.6.2021. godine donosi sledeći:

In accordance with Article 16 of the Law on protection of whistleblowers (“Official Gazette of RS”, no. 128/2014; hereinafter referred to as the “**Law**”) and Rulebook on method for internal whistleblowing, method for designating authorized person of the employer and other issues significant for internal whistleblowing at employer which has more than ten employees (“Official Gazette of RS”, no. 49/2015 and 44/2018; hereinafter referred to as “**Rulebook**”), the company CTP Invest doo Beograd-Novi Beograd with registered seat at the address Bulevar Zorana Djindjica no. 64A, registry number 21287172, tax identification number 110027463, which legal representative is director Richard Wilkinson (hereinafter referred to as the: „**Employer**“), on 7.6.2021 renders the following:

PRAVILNIK O POSTUPKU UNUTRAŠNJEG UZBUNJIVANJA

RULEBOOK ON INTERNAL WHISTLEBLOWING PROCEDURE

I. OSNOVNE ODREDBE

I. GENERAL PROVISIONS

Član 1.

Article 1

Ovim pravilnikom uređuje se postupak unutrašnjeg uzbunjivanja kod Poslodavca, prava zaposlenih po osnovu uzbunjivanja, obaveze i odgovornosti Poslodavca u vezi sa unutrašnjim uzbunjivanjem i druga pitanja vezana za unutrašnje uzbunjivanje kod Poslodavca.

This rulebook governs internal whistleblowing procedure with the Employer, employee's rights in relation to whistleblowing, Employer's obligations and responsibilities pertaining to internal whistleblowing procedure, as well as other issues related to internal whistleblowing procedure with the Employer.

Član 2.

Article 2

Poslodavac, ovlašćeno lice i druga odgovorna lica kod Poslodavca, zaposlena i radno angažovana lica kod Poslodavca, dužni su da se pridržavaju dužnosti i obaveza predviđenih ovim pravilnikom, Zakonom i Pravilnikom.

Employer, authorized person, and other officers in charge with the Employer, employees and other persons who are in working relationship with the Employer are obliged to comply with duties and obligations set forth in this rulebook, Law and Rulebook.

II. ZNAČENJE POJEDINIH POJMOVA

II. INTERPRETATION OF CERTAIN TERMS

Član 3.

Article 3

"Uzbunjivanje" je otkrivanje informacije o kršenju propisa, kršenju ljudskih prava, vršenju javnog ovlašćenja protivno svrsi zbog koje je povereno, opasnosti po život, javno zdravlje, bezbednost, životnu sredinu, kao i radi sprečavanja štete velikih razmera;

„Informacija“ jeste informacija koja može biti predmet uzbunjivanja i koja sadrži podatke o kršenju propisa, kršenju ljudskih prava, vršenju javnih ovlašćenja protivno svrsi zbog koje je povereno, opasnosti po život, javno zdravlje, bezbednost, životnu sredinu, kao i podatke radi sprečavanja štete velikih razmera. Informacija može da sadrži potpis uzbunjivača i podatke o uzbunjivaču;

"Uzbunjivač" je fizičko lice koje izvrši uzbunjivanje u vezi sa svojim radnim angažovanjem, postupkom zapošljavanja, korišćenjem usluga državnih i drugih organa, nosilaca javnih ovlašćenja ili javnih službi, poslovnom saradnjom i pravom vlasništva na privrednom društvu;

„Ovlašćeno lice“ je lice koje je odlukom Poslodavca ovlašćeno za prijem informacije i vođenje postupka unutrašnjeg uzbunjivanja kod Poslodavca;

"Ovlašćeni organ" je organ Republike Srbije, teritorijalne autonomije ili jedinice lokalne samouprave ili nosilac javnih ovlašćenja nadležan da postupa po informaciji kojom se vrši uzbunjivanje, u skladu sa zakonom;

„Unutrašnje uzbunjivanje“ je otkrivanje informacije Poslodavcu;

„Radno angažovanje“ je radni odnos, rad van radnog odnosa, volontiranje, vršenje funkcije, kao i svaki drugi faktički rad za Poslodavca;

"Štetna radnja" je svako činjenje ili nečinjenje u vezi sa uzbunjivanjem kojim se uzbunjivaču ili licu koje ima pravo na zaštitu kao uzbunjivač ugrožava ili povređuje pravo, odnosno kojim se ta lica stavljaju u nepovoljniji položaj.

"Whistleblowing" is disclosure of information on violation of regulations, violation of human rights, exercise of public authority contrary to the purpose for which it was entrusted, threat to life, public health, safety, environment, and prevention of large-scale damage

"Information" is information which may be subject of whistleblowing and which contains data on violation of regulations, breach of human rights, exercising of public authorizations contrary to the purpose for which they have been delegated, hazards to life, public health, safety, environment, as well as data to prevent large-scale damage. The information may include the whistleblower's signature and whistleblower information;

"Whistleblower" is a natural person who performed whistleblowing in terms of his working relationship, employment procedure, use of services rendered by public authorities or other authorities, holders of public authorities or public services, business cooperation, ownership of shares in the company;

"Authorized person" is a person who is authorized to receive information and govern internal whistleblowing procedure with the Employer based on Employer's decision;

"Authorized authority" is any republic, provincial, or local government authority or holder of public authorities competent to act upon the information disclosed by a whistleblower in accordance with the Law;

"Internal whistleblowing procedure" is disclosure of information to Employer;

"Working relationship" is employment, work outside employment, volunteering, exercising post, or any other factual work for an Employer;

"Damaging action" is any action or failure to act related to the whistleblowing which threatens or violates the right of a whistleblower or a person who is entitled to protection as a whistleblower, or which places such persons in an unfavorable position.

III. PRAVO NA ZAŠTITU UZBUNJIVAČA I DRUGIH LICA

Pravo na zaštitu Uzbunjivača

Član 4.

Uzbunjivač ima pravo na zaštitu, u skladu sa Zakonom, ako:

- izvrši Uzbunjivanje kod Poslodavca, Ovlaštenog organa ili javnosti na način propisan Zakonom;
- otkrije informaciju u roku od jedne godine od dana saznanja za izvršenu radnju zbog koje vrši uzbunjivanje, a najkasnije u roku od deset godina od dana izvršenja te radnje;
- bi u trenutku Uzbunjivanja, na osnovu raspoloživih podataka, u istinitost informacije poverovalo lice sa prosečnim znanjem i iskustvom kao i Uzbunjivač.

Pravo na zaštitu drugih lica

Član 5.

Povezano lice ima pravo na zaštitu kao Uzbunjivač, ako učini verovatnim da je prema njemu preduzeta Štetna radnja zbog povezanosti sa Uzbunjivačem

Član 6.

Pravo na zaštitu kao Uzbunjivač ima lice koje učini verovatnim da je prema njemu preduzeta Štetna radnja, ako je lice koje je preduzelo Štetnu radnju pogrešno smatralo da je to lice Uzbunjivač, odnosno povezano lice.

Član 7.

Lice koje traži podatke u vezi sa Informacijom ima pravo na zaštitu kao Uzbunjivač ako učini verovatnim da je prema njemu preduzeta Štetna radnja zbog traženja tih podataka.

III. RIGHT TO PROTECTION OF WHISTLEBLOWERS AND OTHER PERSONS

Whistleblower's right to protection

Article 4

The whistleblower is entitled to protection, in accordance with the Law, if:

- executes Whistleblowing with the Employer, the competent authority or the public in the manner prescribed by the Law;
- discloses information within one year from the date from the day he/she learned about the committed action and no later than 10 years from the commission of such action;
- at the time of Whistleblowing, based on the available data, another person with average knowledge and experience similar to the person making a disclosure would believe that the disclosure is true.

Right to protection of other persons

Article 5

Associated person has the right to protection same as Whistleblower if he/she made probable that Damaging action has been undertaken against him/her due to association with Whistleblower.

Article 6

The right to protection as a Whistleblower, shall have a person that made probable that Damaging action has been undertaken against him by the person undertaking Damaging action due to erroneous believes of the latter that such person is a Whistleblower or associated person.

Article 7

The person that request data in relation to Information has the right same as Whistleblower if he/she made probable that Damaging action has been undertaken against him/her due to request of such information.

Član 8.

Lice koje je u vršenju službene dužnosti dostavilo Informaciju ima pravo na zaštitu kao Uzbunjivač ako učini verovatnim da je prema njemu preduzeta štetna radnja zbog dostavljanja Informacije.

Zaštita podataka o ličnosti Uzbunjivača**Član 9.**

Ovlašćeno lice je dužno da štiti podatke o ličnosti Uzbunjivača, odnosno podatke na osnovu kojih se može otkriti identitet Uzbunjivača, osim ako se Uzbunjivač ne saglasi sa otkrivanjem tih podataka, a u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti.

Svako lice koje sazna podatke iz stava 1. ovog člana dužno je da štiti te podatke.

Ovlašćeno lice je dužno da prilikom prijema informacije obavesti Uzbunjivača da njegov identitet može biti otkriven nadležnom organu, ako bez otkrivanja identiteta Uzbunjivača ne bi bilo moguće postupanje tog organa, kao i da ga obavesti o merama zaštite učesnika u krivičnom postupku.

Ovlašćeno lice je dužno da pre otkrivanja identiteta obavesti Uzbunjivača o tome, ako je u toku postupka unutrašnjeg uzbunjivanja neophodno da se otkrije identitet Uzbunjivača.

Podaci iz stava 1. ovog člana ne smeju se saopštiti licu na koje se ukazuje u Informaciji, ako zakonom nije drugačije propisano.

Article 8

The person who submitted Information while exercising official competence has the right to protection same as Whistleblower if he/she made probable that Damaging action has been undertaken against him/her due to request of such information.

Whistleblower's data protection**Article 9**

Authorized person is obliged to protect Whistleblower's personal data, i.e. data which may reveal the identity of a Whistleblower, except in case where a Whistleblower agrees with disclosure of such data, in accordance with the law governing personal data protection.

Any person who comes into possession of data referred to in paragraph 1 of this Article, shall protect such data.

Authorized person is obliged to, while receiving information, inform a Whistleblower that his identity may be revealed to the competent authority, if the actions of that authority would not otherwise be possible, and inform him about protection measures of participants in criminal proceedings.

If it is necessary to reveal the identity of a Whistleblower in the course of internal whistleblowing procedure, Authorized person is obliged to inform the Whistleblower about it before revealing his identity.

Personal data referred to in paragraph 1 of this Article shall not be revealed to a person to whom the disclosure referred in Information except where a special law provides otherwise.

IV. PRAVA I OBAVEZE POSLODAVCA I Uzbunjivača u vezi sa Uzbunjivanjem

Zabrana sprečavanja Uzbunjivanja i preduzimanja Štetne radnje

Član 10.

Zabranjeno je sprečavanje Uzbunjivanja i preduzimanje Štetne radnje prema zaposlenom.

Zabrana stavljanja uzbunjivača u nepovoljniji položaj

Član 11.

Poslodavac ne sme činjenjem ili nečinjenjem da stavi Uzbunjivača u nepovoljniji položaj u vezi sa Uzbunjivanjem, a naročito ako se nepovoljniji položaj odnosi na: zapošljavanje; sticanje svojstva pripravnika ili volontera; rad van radnog odnosa; obrazovanje, osposobljavanje ili stručno usavršavanje; napredovanje na poslu, ocenjivanje, sticanje ili gubitak zvanja; disciplinske mere i kazne; uslove rada; prestanak radnog odnosa; zaradu i druge naknade iz radnog odnosa; učešće u dobiti Poslodavca; isplatu nagrade i otpremnine; raspoređivanje ili premeštaj na drugo radno mesto; nepreduzimanje mera radi zaštite zbog uznemiravanja od strane drugih lica; upućivanje na obavezne zdravstvene preglede ili upućivanje na preglede radi ocene radne sposobnosti.

Obaveze Poslodavca

Član 12.

Poslodavac je dužan da svim zaposlenima i drugim radno angažovanim licima kod Poslodavca dostavi pismeno obaveštenje o pravima po osnovu Uzbunjivanja.

Poslodavac je dužan da odlukom odredi Ovlašćeno lice.

IV. RIGHTS AND DUTIES OF WHISTLEBLOWER AND EMPLOYER IN RELATION TO WHISTLEBLOWING

Prohibition of prevention of Whistleblowing and performing Damaging action

Article 10

Prevention of Whistleblowing and performance of Damaging action towards employee is prohibited.

Prohibition of placing the whistleblower in a less favorable position

Article 11

The Employer must not, by performing actions or not performing any actions, place Whistleblower in a less favorable position related to the Whistleblowing, especially if the less favorable position relates to employment procedure; getting the status of an intern or a volunteer; work outside employment; education, training and professional development; promotion at work, appraisal, acquisition or loss of position; disciplinary measures and penalties; working conditions; termination of employment; share in the profits of the Employer; payment premium and severance pay; deployment or transfer to another job; failure to take measures to protect a whistleblower from harassment by others; referral to the mandatory medical examinations or referral to examinations to assess the work capacity.

Employer's obligations

Article 12

The Employer is obliged to deliver to all employees and all other persons in working relationship written notification on rights based on Whistleblowing.

The Employer is obliged to appoint by its decision Authorized person.

Poslodavac je dužan da ovaj pravilnik istakne na vidnom mestu, dostupnom svakom radno angažovanom licu, kao i na internet stranici Poslodavca ako postoje tehničke mogućnosti.

The Employer is obliged to publish this rulebook at visible place, reachable to each person in working relationship, as well as to publish on web site address of Employer if technical possibilities allow that.

Pravo na naknadu štete zbog Uzbunjivanja

Damage compensation due to Whistleblowing

Član 13.

Article 13

U slučaju nanošenja štete zbog Uzbunjivanja, Uzbunjivač ima pravo na naknadu štete, u skladu sa zakonom koji uređuje obligacione odnose.

In cases of inflicting damaging consequences due to Whistleblowing, a Whistleblower shall have the right to compensation for damage in accordance with the law regulating contract and torts.

Pravo na sudsku zaštitu Uzbunjivača

Court protection of Whistleblower

Član 14

Article 14

Uzbunjivač prema kome je preduzeta Štetna radnja u vezi sa Uzbunjivanjem ima pravo na sudsku zaštitu.

Whistleblower to whom the Damaging action has been performed in relation to Whistleblowing has the right to court protection.

Sudska zaštita se ostvaruje podnošenjem tužbe za zaštitu u vezi sa Uzbunjivanjem nadležnom sudu, u roku od šest meseci od dana saznanja za preduzetu Štetnu radnju, odnosno tri godine od dana kada je Štetna radnja preduzeta.

Court protection is exercised by submission of a lawsuit before a competent court within 6 months from the day of learning about the Damaging action undertaken, or 3 years from the day of the occurrence of a damaging consequence.

Tužbom za zaštitu u vezi sa Uzbunjivanjem može se tražiti:

By submission of lawsuit in relation to Whistleblowing, the following may be requested:

- utvrđenje da je prema Uzbunjivaču preduzeta Štetna radnja;
- zabrana vršenja i ponavljanja Štetne radnje;
- uklanjanje posledica Štetne radnje;
- naknada materijalne i nematerijalne štete; i
- objavljivanje presude donete po tužbi podnetoj u vezi sa Uzbunjivanjem u sredstvima javnog informisanja, o trošku tuženog.
- determinacija da Damaging action has been undertaken towards Whistleblower;
- prohibition of performance and repeat of Damaging action;
- elimination of the consequences of Damaging action;
- compensation of material and non-material damage; and
- publishing of decision rendered upon submitted lawsuit in relation to Whistleblowing in the media, per the cost of respondent.

Tužbom za zaštitu u vezi sa Uzbunjivanjem ne može se pobijati zakonitost pojedinačnog akta Poslodavca kojim je rešavano o pravima, obavezama i odgovornostima radno angažovanog lica kod Poslodavca po osnovu rada.

By virtue of lawsuit in relation to Whistleblowing it cannot be challenged the legality of an individual act of the Employer based on which it has been decided on rights, obligations and responsibilities of person in working relationship with the

Employer on the basis of employment engagement.

U tužbi za ocenu zakonitosti pojedinačnog akta Poslodavca kojim je rešavano o pravima, obavezama i odgovornosti Uzbunjivača po osnovu rada, po posebnim propisima, Uzbunjivač može istaći navod da pojedinačni akt Poslodavca predstavlja Štetnu radnju u vezi sa Uzbunjivanjem, u skladu sa Zakonom.

In the lawsuit on assessment of legality of Employer's individual act by virtue of which it has been decided on rights, obligations and responsibilities of Whistleblower based on employment engagement, on the ground of special regulations, the Whistleblower may raise a notion that Employer's individual act represents Damaging action pertaining to Whistleblowing, in accordance with the Law.

U postupku zaštite u vezi sa Uzbunjivanjem ili u postupku za ocenu zakonitosti pojedinačnog akta Poslodavca, sud koji vodi postupak može odrediti privremenu meru u skladu sa zakonom.

In the procedure pertaining to protection related to Whistleblowing or in procedure for assessment of legality of the Employer's individual act, the court governing procedure may impose temporary injunction in accordance with the law.

Zabrana zloupotrebe uzbunjivanja

Prohibition against Abuse of Whistleblowing

Član 15

Article 15

Zabranjena je zloupotreba Uzbunjivanja.

Abuse of Whistleblowing is prohibited.

Zloupotrebu Uzbunjivanja vrši lice koje dostavi Informaciju za koju je znalo da nije istinita ili koje pored zahteva za postupanje u vezi sa Informacijom kojom se vrši Uzbunjivanje traži protivpravnu korist

Abuse of Whistleblowing commits a person who: discloses information he knew was untrue; in addition to request to act upon Information considered Whistleblowing, requires unlawful benefit.

V. POSTUPAK UNUTRAŠNJEG UZBUNJIVANJA

V. INTERNAL WHISTLEBLOWING PROCEDURE

Pokretanje postupka

Initiation of procedure

Član 16

Article 16

Postupak unutrašnjeg uzbunjivanja započinje dostavljanjem Informacije Poslodavcu. Jasnoće radi Informacija se može dostaviti Poslodavcu i u slučaju kada je radno angažovanim licima poznato i/ili sumnjaju da su učinjene povrede opisane u Pravilima i preporukama uzbunjivanja usvojenim na nivou CTP Grupe društava (u daljem tekstu: „Pravila Grupe“) prema važećoj verziji objavljenoj na intranet stranici na nivou CTP Grupe:

A procedure of internal whistleblowing is initiated by making a disclosure to an Employer. For the avoidance of any doubt, the Information may be submitted to Employer in case that person in working relationship is aware of or suspects that violations described in Guidelines and Group Whistleblower Policy which are accepted on the level of CTP Group Companies (hereinafter referred to as the „Group Policies“) are also committed, according to the valid version published

<https://intranet.ctp.eu/web/guest/whistleblowing>

on the following web address on the level of CTP Group:

<https://intranet.ctp.eu/web/guest/whistleblowing>.

Dostavljanje Informacije vrši se Ovlašćenom licu pismeno ili usmeno.

The delivery of Information is to be made to Authorized person in writing or orally.

Nezavisno od navedenog, radno angažovana lica kod Poslodavca imaju pravo da podnesu anonimnu prijavu Informacije u skladu sa članom 20 pravilnika.

Notwithstanding the above, persons in working relationship with the Employer are also entitled to submit anonymous report in accordance with the Article 20 of this rulebook.

Poslodavac je dužan da u svakom slučaju (bez obzira na gore opisani način dostavljanja Informacije) postupi po Informaciji bez odlaganja, a najkasnije u roku od 15 dana od dana prijema Informacije.

Anyhow (regardless of the above described manner of submission of Information), the Employer shall act upon receiving Information without delay, but within 15 days from the day the disclosure was received by latest.

Dostavljanje Informacije

Delivery of Information

Član 17.

Article 17

Pismeno dostavljanje Informacije može se učiniti neposrednom predajom pismena o informaciji u vezi sa unutrašnjim uzbunjivanjem, običnom ili preporučenom pošiljkom, kao i elektronskom poštom na e-mail Ovlašćenog lica, ukoliko postoje tehničke mogućnosti i u skladu sa zakonom.

Written submission of Information can be done by direct delivery of written Information on internal Whistleblowing, ordinary or registered mail, as well as by sending an e-mail to the Authorized person's email, if there are technical possibilities and in accordance with the law.

Usmeno dostavljanje Informacije vrši se usmeno na zapisnik.

Delivery of oral Information is to be done as a transcript of a verbal statement.

Zapisnik o usmeno dostavljenoj Informaciji sadrži sve potrebne podatke u skladu sa Zakonom i Pravilnikom.

Transcript in relation to verbal statement contains all required data in accordance with the Law and Rulebook.

Član 18

Article 18

Obične i preporučene pošiljke na kojima je označeno da se upućuju Ovlašćenom licu ili na kojima je vidljivo na omotu da se radi o Informaciji u vezi sa unutrašnjim Uzbunjivanjem može da otvori samo Ovlašćeno lice.

Ordinary and registered items marked to be sent to the Authorized person or showing on the package that it is Information related to the Whistleblowing may only be opened by an Authorized person.

Potvrda o prijemu Informacije

Confirmation on receipt of Information

Član 19.

Article 19

Prilikom dostavljanja Informacije, Ovlašćeno lice sastavlja potvrdu o prijemu Informacije u vezi sa unutrašnjim Uzbunjivanjem u skladu sa Zakonom i Pravilnikom.

While submitting Information, the Authorized person drafts confirmation on receipt of Information in relation to internal Whistleblowing in accordance with the Law and Rulebook.

Potvrda o prijemu Informacije u vezi sa unutrašnjim Uzbunjivanjem sadrži: kratak opis činjeničnog stanja o Informaciji u vezi sa unutrašnjim Uzbunjivanjem; vreme, mesto i način dostavljanja Informacije u vezi sa unutrašnjim Uzbunjivanjem; broj i opis priloga podnetih uz Informaciju o unutrašnjem Uzbunjivanju; podatke o tome da li Uzbunjivač želi da podaci o njegovom identitetu ne budu otkriveni; podatke o Poslodavcu i potpis Ovlašćenog lica.

Confirmation on receipt of Information pertaining to internal Whistleblowing contains: short description of factual state on Information pertaining to internal Whistleblowing; date, place and manner of submission of Information in relation to internal Whistleblowing, number and description of appendices submitted with Information on internal Whistleblowing; data on whether the Whistleblower desires his/her data on identity not to be revealed; data on Employer and signature of Authorized person.

Potvrda o prijemu Informacije u vezi sa unutrašnjim Uzbunjivanjem može da sadrži potpis Uzbunjivača i podatke o Uzbunjivaču, ukoliko on to želi.

Confirmation on receipt of Information pertaining to internal Whistleblowing may contain Whistleblower's signature and data on Whistleblower if he/she desires.

Anonimne prijave

Anonymous reports

Član 20.

Article 20

Uzbunjivač može takođe da izvrši prijavu i na anonimnan način, u kom slučaju će koristiti poseban kanal za uzbunjivanje dostupan na internoj platformi za uzbunjivanje objavljenoj na sledećoj intranet stranici na nivou CTP Grupe: www.intranet.ctp.eu, na način bliže opisan Pravilima Grupe.

The Whistleblower may also submit report anonymously, in which case he/she shall use a special channel for whistleblowing available on intranet whistleblowing platform published on the following web address on the level of CTP Group: www.intranet.ctp.eu, per the manner more closely defined under the Group Policies.

Poslodavac je dužan da postupa po anonimnim obaveštenjima u vezi sa Informacijom u okviru svojih ovlašćenja i ne sme preduzimati mere radi otkrivanja identiteta Uzbunjivača.

The Employer is obliged to, within its powers, act on anonymous notifications related to Information and it must not perform actions in regard to revealing identity of anonymous Whistleblower.

U slučaju anonimne prijave, Ovlašćeno lice, zbog nepoznatog identiteta Uzbunjivača, ne omogućava uvid u spise predmeta, prisustvovanje radnjama u toku postupka, niti obaveštava Uzbunjivača o preduzetim radnjama po prijavi i ne dostavlja mu izveštaj u skladu sa članom 21 pravilnika.

In case of anonymous, the Authorized person, due to unknown Whistleblower's identity, will not enable review of case files, attending actions in the course of procedure, nor it shall inform Whistleblower in regard to actions performed upon submitted report and will not issue to Whistleblower report in accordance with article 21 of the rulebook.

Postupanje po Informaciji

Acting on upon Information

Član 21

Po okončanju postupka unutrašnjeg Uzbunjivanja, Ovlašćeno lice u roku od 15 dana:

- sastavlja izveštaj o preduzetim radnjama u postupku unutrašnjeg Uzbunjivanja; i
- predlaže mere radi otklanjanja utvrđenih nepravilnosti i posledica Štetne radnje nastalih u vezi sa unutrašnjim Uzbunjivanjem.

Član 22

Izveštaj o preduzetim radnjama u postupku unutrašnjeg Uzbunjivanja sadrži sve potrebne podatke u skladu sa zakonom i dostavlja se Poslodavcu i Uzbunjivaču.

Uzbunjivač može da se izjasni na izveštaj iz stava 1. ovog člana u roku od 8 dana od dana prijema takvog izveštaja.

Obaveze Poslodavca u postupku unutrašnjeg Uzbunjivanja

Član 23

Poslodavac je dužan da, na zahtev Uzbunjivača, pruži obaveštenja Uzbunjivaču o toku i radnjama preduzetim u postupku unutrašnjeg Uzbunjivanja, kao i da omogući Uzbunjivaču da izvrši uvid u spise predmeta i da prisustvuje radnjama u postupku.

Poslodavac je dužan da, u okviru svojih ovlašćenja, preduzme mere radi otklanjanja utvrđenih nepravilnosti u vezi sa Informacijom.

Poslodavac je dužan da, u okviru svojih ovlašćenja, zaštititi Uzbunjivača od Štetne radnje, kao i da preduzme neophodne mere radi obustavljanja Štetne radnje i otklanjanja posledica Štetne radnje.

Poslodavac je dužan da obavesti Uzbunjivača o ishodu postupka unutrašnjeg Uzbunjivanja, po njegovom okončanju, u roku od 15 dana od dana okončanja postupka unutrašnjeg Uzbunjivanja.

Article 21

Upon finishing internal Whistleblowing procedure, the Authorized person within 15 days' deadline:

- drafts report on performed actions in the internal Whistleblowing procedure; and
- suggests measures for the purpose of eliminating determined irregularities and consequences of Damaging actions occurred in relation to internal Whistleblowing.

Article 22

Report on performed actions in the internal Whistleblowing procedure contains all relevant data in line with the law and is to be submitted to Employer and Whistleblower.

The Whistleblower is entitled to reply to report outlined in paragraph 1 of this article within 8 days as of the date of receipt of such report.

Employer's obligation in internal Whistleblowing procedure

Article 23

Upon request of Whistleblower, the Employer is obliged to submit notice to Whistleblower in relation to course and performed actions in the internal Whistleblowing procedure, as well as to enable to Whistleblower to review the case files and attend actions in the procedure.

The Employer is obliged to, within its powers, perform measures in order to eliminate determined irregularities pertaining to Information.

The Employer is obliged to, within its powers, protect Whistleblower from Damaging action, as well as to perform measures necessary for the suspension of Damaging action and elimination of its consequences.

The Employer is obliged to notify the Whistleblower in relation to success of internal Whistleblowing procedure, upon its closure, within 15 days since the closure of the internal Whistleblowing procedure.

Postupak unutrašnjeg uzbunjivanja ako su u informaciji sadržani tajni podaci

Whistleblowing when a Disclosure Contains Classified Data

Član 24

Article 24

Informacija može da sadrži tajne podatke.

A disclosure may contain confidential data.

Pod tajnim podacima iz stava 1. ovog člana smatraju se podaci koji su u skladu sa propisima o tajnosti podataka prethodno označeni kao tajni.

Classified data referred to in paragraph 1 of this Article are those considered classified in accordance with the regulations on classified data.

Ako su u informaciji sadržani tajni podaci, uzbunjivač je dužan da se prvo obrati Poslodavcu, a ako se informacija odnosi na lice koje je ovlašćeno da postupa po informaciji, informacija se podnosi rukovodiocu Poslodavca.

If such disclosure contains classified data, a whistleblower shall first address his employer, and if a disclosure refers to a person authorized to act upon disclosures, such disclosure shall be made to the immediate supervisor of that person.

U slučaju da Poslodavac nije u roku od 15 dana postupio po informaciji u kojoj su sadržani tajni podaci, odnosno ako nije odgovorio ili nije preduzeo odgovarajuće mere iz svoje nadležnosti, Uzbunjivač se može obratiti Ovlašćenom organu.

In case that the Employer failed to act upon disclosure containing classified information within 15 days or fails to respond or take appropriate measures within his authority, the Whistleblower may contact the Authorized authority.

Izuzetno od stava 3. ovog člana, u slučaju da se informacija odnosi na rukovodioca Poslodavca, informacija se podnosi Ovlašćenom organu.

Notwithstanding paragraph 3 of this Article, in case a disclosure refers to a manager within the Employer, such disclosure shall be made to an Authorized authority.

Ako su u informaciji sadržani tajni podaci, Uzbunjivač ne može uzbuniti javnost, ako zakonom nije drugačije određeno.

If a disclosure contains classified information, a Whistleblower cannot make it public, unless the law provides otherwise.

Ako su u informaciji sadržani tajni podaci, Uzbunjivač i druga lica su dužni da se pridržavaju opštih i posebnih mera zaštite tajnih podataka propisanih zakonom koji uređuje tajnost podataka.

If a disclosure contains classified information, a whistleblower and other persons shall comply with general and special measures for protection of classified data.

VI. ZAVRŠNE ODREDBE

VI. CLOSING PROVISIONS

Član 25

Article 25

Na slučajeve koji nisu uređeni ovim pravilnikom primenjuju se neposredno odredbe Zakona, Pravilnika, drugih primenljivih propisa i Pravila Grupe. U slučaju bilo kakvih nesaglasnosti

For every matter that is not defined by this rule-book, the provisions of the Law, Rulebook, other applicable regulations and Group Policies, will be applied. In case of any discrepancies between

između Pravila Grupe i ovog pravilnika, primenjivaće se odredbe ovog pravilnika kao merodavne.

Group Policies and this rulebook, the relevant provisions of this rulebook shall take a precedence.

Ovaj pravilnik se potpisuje dvojezično, na srpskom i na engleskom jeziku. U slučaju bilo kakve nesaglasnosti između ove dve verzije, verzija na srpskom će biti merodavna.

This rulebook is executed bilingually in Serbian and English language. In case of any inconsistency between the two versions, the Serbian version shall prevail.

Ova odluka stupa na snagu osmog dana od dana objavljivanja na oglasnoj tabli Poslodavca.

This rulebook shall become effective on the eighth day from the day of its publication on the bulletin board of the Employer.

U Beogradu/In Belgrade dana/on 7.6.2021.

Za Poslodavca / On behalf of the Employer


Richard Wilkinson
Direktor / Director



U SKLADU SA ČLANOM 14 STAV 4
ZAKONA O ZAŠTITI UZBUNJIVAČA ("SL.
GLASNIK RS", BR. 128/2014),

POSLODAVAC: CTP Invest doo Beograd –
Novi Beograd, Bulevar Zorana Đinđića broj
64a, matični broj 21287172

Dana _____ godine daje
ZAPOSLENOM _____ sledeće:

OBAVEŠTENJE

Zakonom o zaštiti uzbunjivača se uređuje uzbunjivanje, postupak uzbunjivanja, prava uzbunjivača, obaveza državnih i drugih organa i organizacija i pravnih i fizičkih lica u vezi sa uzbunjivanjem, kao i druga pitanja od značaja za uzbunjivanje i zaštitu uzbunjivača.

Značenje izraza

U smislu ovog zakona, pojedini izrazi imaju sledeće značenje:

- 1) "uzbunjivanje" je otkrivanje informacije o kršenju propisa, kršenju ljudskih prava, vršenju javnog ovlašćenja protivno svrsi zbog koje je povereno, opasnosti po život, javno zdravlje, bezbednost, životnu sredinu, kao i radi sprečavanja štete velikih razmera;
- 2) "uzbunjivač" je fizičko lice koje izvrši uzbunjivanje u vezi sa svojim radnim angažovanjem, postupkom zapošljavanja, korišćenjem usluga državnih i drugih organa, nosilaca javnih ovlašćenja ili javnih službi, poslovnom saradnjom i pravom vlasništva na privrednom društvu;
- 3) "poslodavac" je organ Republike Srbije, teritorijalne autonomije ili jedinice lokalne samouprave, nosilac javnih ovlašćenja ili javna služba, pravno lice ili preduzetnik koji radno angažuje jedno ili više lica;
- 4) "odgovorno lice" je lice kome su u pravnom licu povereni određeni poslovi koji se odnose na upravljanje, poslovanje ili proces rada, kao i lice koje u državnom organu, organu teritorijalne autonomije i jedinice lokalne samouprave vrši određene dužnosti;
- 5) "radno angažovanje" je radni odnos, rad van radnog odnosa, volontiranje, vršenje

PURSUANT TO ARTICLE 14 PARAGRAPH
4 OF THE LAW ON WHISTLERBLOWERS
PROTECTION ("RS OFFICIAL GAZETTE",
NO. 128/2014),

EMPLOYER: CTP Invest doo Beograd-Novi
Beograd, Bulevar Zorana Djindjica no. 64a,
registration number 21287172,

on _____ delivers to EMPLOYEE
_____ the following:

NOTIFICATION

The Law on Whistleblowers Protection regulates whistleblowing, whistleblowing procedure, rights of whistleblowers, obligations of the state authorities and other authorities and organizations in relation to whistleblowing, as well as other issues of importance for whistleblowing and protection of whistleblowers.

Definitions

In terms of this Law, terms shall have the following meaning:

- 1) "whistleblowing" is disclosure of information on violation of regulations, violation of human rights, exercise of public authority contrary to the purpose for which it was entrusted, threat to life, public health, safety, environment, and prevention of large-scale damage;
- 2) "whistleblower" is a natural person who performed whistleblowing in terms of his working relationship, employment procedure, use of services rendered by public authorities or other authorities, holders of public authorities or public services, business cooperation, ownership of shares in the company;
- 3) "employer" is an authority of the Republic of Serbia, territorial province or local self-government unit, holder of public authorities or a public service, or legal entity or entrepreneur which employs one or more persons;
- 4) "responsible person" is a person in the legal entity entrusted with certain duties relating to management, operations and workflow, as well as a person who performs certain duties in the state authority,

funkcije, kao i svaki drugi faktički rad za poslodavca;

6) "ovlašćeni organ" je organ Republike Srbije, teritorijalne autonomije ili jedinice lokalne samouprave ili nosilac javnih ovlašćenja nadležan da postupa po informaciji kojom se vrši uzbunjivanje, u skladu sa zakonom;

7) "štetna radnja" je svako činjenje ili nečinjenje u vezi sa uzbunjivanjem kojim se uzbunjivaču ili licu koje ima pravo na zaštitu kao uzbunjivač ugrožava ili povređuje pravo, odnosno kojim se ta lica stavljaju u nepovoljniji položaj.

territorial province and local government unit.

5) "working relationship" is employment, work outside employment, volunteering, exercising post, or any other factual work for an employer;

6) "authorized authority" is any republic, provincial, or local government authority or holder of public authorities competent to act upon the information disclosed by a whistleblower in accordance with the Law;

7) "damaging action" is any action or failure to act related to the whistleblowing which threatens or violates the right of a whistleblower or a person who is entitled to protection as a whistleblower, or which places such persons in an unfavorable position.

Zabrana sprečavanja uzbunjivanja

Zabranjeno je sprečavanje uzbunjivanja. Odredba opšteg akta ili pojedinačnog akta kojom se sprečava uzbunjivanje je ništava. Zabranjeno je preduzimanje štetne radnje.

Prohibition against Prevention of Whistleblowing

Prevention of whistleblowing is prohibited. The provision of a general act or an individual act which prevents whistleblowing shall be null and void. It is prohibited to undertake damaging action.

Pravo na zaštitu uzbunjivača

Uzbunjivač ima pravo na zaštitu, u skladu sa zakonom, ako:

1) izvrši uzbunjivanje kod poslodavca, ovlašćenog organa ili javnosti na način propisan zakonom;

2) otkrije informaciju iz člana 2. tačka 1) zakona (u daljem tekstu: informacija) u roku od jedne godine od dana saznanja za izvršenu radnju zbog koje vrši uzbunjivanje, a najkasnije u roku od deset godina od dana izvršenja te radnje;

3) bi u trenutku uzbunjivanja, na osnovu raspoloživih podataka, u istinitost informacije, poverovalo lice sa prosečnim znanjem i iskustvom kao i uzbunjivač.

Right to Protection of Whistleblower

The whistleblower is entitled to protection, in accordance with the Law, if:

1) executes whistleblowing with the employer, the competent authority or the public in the manner prescribed by the law;

2) discloses information referred to in Article 2, item 1) of the Law (hereinafter: the disclosure) within one year from the date within one year from the day he learned about the committed action and no later than 10 years from the commission of such action;

3) at the time of whistleblowing, based on the available data, another person with average knowledge and experience similar to the person making a disclosure would believe that the disclosure is true.

Pravo na zaštitu zbog pogrešnog označavanja uzbunjivača

Pravo na zaštitu kao uzbunjivač, ima lice koje učini verovatnim da je prema njemu preduzeta štetna radnja, ako je lice koje je

The right to protection due to incorrect indication of whistleblower

The right to protection as a whistleblower, shall have a person that made probable that damaging action has been undertaken

preduzelo štetnu radnju, pogrešno smatralo da je to lice uzbunjivač, odnosno povezano lice.

against him by the person undertaking damaging action due to erroneous believes of the latter that such person is a whistleblower or associated person.

Zaštita podataka o ličnosti uzbunjivača

Protection of a Whistleblower's Personal Data

Lice koje je ovlašćeno za prijem informacije dužno je da, štiti podatke o ličnosti uzbunjivača, odnosno podatke na osnovu kojih se može otkriti identitet uzbunjivača, osim ako se uzbunjivač ne saglasi sa otkrivanjem tih podataka, a u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti.

A person authorized to receive disclosures shall, upon request by a whistleblower, protect the whistleblower's personal data or data which may reveal the identity of a whistleblower, except in case where a whistleblower agrees with disclosure of such data, in accordance with the law governing personal data protection.

Svako lice koje sazna podatke iz stava 1. ovog člana, dužno je da štiti te podatke.

Any person who comes into possession of data referred to in paragraph 1 of this Article, shall protect such data.

Lice ovlašćeno za prijem informacije dužno je da prilikom prijema informacije, obavesti uzbunjivača da njegov identitet može biti otkriven nadležnom organu, ako bez otkrivanja identiteta uzbunjivača ne bi bilo moguće postupanje tog organa, kao i da ga obavesti o merama zaštite učesnika u krivičnom postupku.

A person authorized to receive disclosures shall, while receiving information, inform a whistleblower that his identity may be revealed to the competent authority, if the actions of that authority would not otherwise be possible, and inform him about protection measures of participants in criminal proceedings.

Ako je u toku postupka neophodno da se otkrije identitet uzbunjivača, lice ovlašćeno za prijem informacije dužno je da o tome, pre otkrivanja identiteta, obavesti uzbunjivača.

If it is necessary to reveal the identity of a whistleblower in the course of proceedings, a person authorized to receive disclosures shall inform the whistleblower about it before revealing his identity.

Podaci iz stava 1. ovog člana ne smeju se saopštiti licu na koje se ukazuje u informaciji, ako posebnim zakonom nije drugačije propisano

Personal data referred to in paragraph 1 of this Article shall not be revealed to a person to whom the disclosure referred in information except where a special law provides otherwise.

Zabrana zloupotrebe uzbunjivanja

Prohibition against Abuse of Whistleblowing

Zabranjena je zloupotreba uzbunjivanja. Zloupotrebu uzbunjivanja vrši lice koje dostavi informaciju za koju je znalo da nije istinita; pored zahteva za postupanje u vezi sa informacijom kojom se vrši uzbunjivanje traži protivpravnu korist.

Abuse of whistleblowing is prohibited. Abuse of whistleblowing commits a person who: discloses information he knew was untrue; in addition to request to act upon information considered whistleblowing, requires unlawful benefit.

Vrste uzbunjivanja

Types of Whistleblowing

Uzbunjivanje može biti unutrašnje, spoljašnje ili uzbunjivanje javnosti.

Whistleblowing may be internal, external, or to the public.

Unutrašnje uzbunjivanje je otkrivanje informacije poslodavcu.

Spoljašnje uzbunjivanje je otkrivanje informacije ovlašćenom organu.

Uzbunjivanje javnosti je otkrivanje informacije sredstvima javnog informisanja, putem interneta, na javnim skupovima ili na drugi način kojim se obaveštenje može učiniti dostupnim javnosti.

Internal whistleblowing is making a disclosure to an employer.

External whistleblowing is making a disclosure to an authorized authority.

Whistleblowing to the public is making a disclosure through the mass media, internet, at public gatherings, or in any other way a disclosure may be made public.

Sadržina informacije

Informacija sadrži podatke o kršenju propisa, kršenju ljudskih prava, vršenju javnog ovlašćenja protivno svrsi zbog koje je povereno, opasnosti po život, javno zdravlje, bezbednost, životnu sredinu, kao i podatke radi sprečavanja štete velikih razmera.

Informacija može da sadrži potpis uzbunjivača i podatke o uzbunjivaču.

Poslodavac i ovlašćeni organ dužni su da postupaju i po anonimnim obaveštenjima u vezi sa informacijom, u okviru svojih ovlašćenja. Anonimne prijave podnose na način bliže opisan Pravilnikom o postupku unutrašnjeg uzbunjivanja Poslodavca.

Contents of Disclosure

The disclosure must contain data on violations of regulations, violation of human rights, exercise of public authority contrary to the purpose for which it was entrusted, threat to life, public health, safety, environment, as well as data preventing large-scale damages.

The disclosure may contain the signature of and data on the whistleblower.

An employer or an authorized authority shall act upon anonymous disclosures within their authorities. Anonymous reports will have to be submitted in the manner more closely outlined in Rulebook on internal whistleblowing procedure of the Employer.

Unutrašnje uzbunjivanje

Obaveze poslodavca

Poslodavac je dužan da, u okviru svojih ovlašćenja, preduzme mere radi otklanjanja utvrđenih nepravilnosti u vezi sa informacijom.

Poslodavac je dužan da, u okviru svojih ovlašćenja, zaštiti uzbunjivača od štetne radnje, kao i da preduzme neophodne mere radi obustavljanja štetne radnje i otklanjanja posledica štetne radnje.

Poslodavac ne sme preduzimati mere u cilju otkrivanja identiteta anonimnog uzbunjivača.

Poslodavac je dužan da svim radno angažovanim licima dostavi pismeno obaveštenje o pravima iz ovog zakona.

Poslodavac je dužan da odredi lice ovlašćeno za prijem informacije i vođenje postupka u vezi sa uzbunjivanjem.

Internal Whistleblowing

Obligations of Employer

The employer is obliged, within his authority, to take measures to eliminate the established irregularities related to disclosure.

The employer shall, within his authority, protect whistleblower from any damaging action, and shall take necessary measures to suspend any damaging action and eliminate the consequences thereof.

The employer shall not take measures in order to reveal the identity of an anonymous whistleblower.

The employer shall deliver to every person in a working relationship with him a written notification of rights under this Law.

The employer shall appoint a person authorized to receive disclosures and to conduct procedure related to the whistleblowing.

Postupak

Procedure

Postupak unutrašnjeg uzbunjivanja započinje dostavljanjem informacije poslodavcu.

Poslodavac je dužan da postupi po informaciji bez odlaganja, a najkasnije u roku od 15 dana od dana prijema informacije.

Poslodavac je dužan da obavesti uzbunjivača o ishodu postupka po njegovom okončanju, u roku od 15 dana od dana okončanja postupka iz stava 1. ovog člana.

Poslodavac je dužan da, na zahtev uzbunjivača, pruži obaveštenja uzbunjivaču o toku i radnjama preduzetim u postupku, kao i da omogući uzbunjivaču da izvrši uvid u spise predmeta i da prisustvuje radnjama u postupku

Uzbunjivanje javnosti

Javnost se može uzbuniti, bez prethodnog obaveštavanja poslodavca ili ovlašćenog organa u slučaju neposredne opasnosti po život, javno zdravlje, bezbednost, životnu sredinu, od nastanka štete velikih razmera, odnosno ako postoji neposredna opasnost od uništenja dokaza.

Prilikom uzbunjivanja javnosti uzbunjivač je dužan da poštuje pretpostavku nevinosti okrivljenog, pravo na zaštitu podataka o ličnosti, kao i da ne ugrožava vođenje sudskog postupka.

Uzbunjivanje ako su u informaciji sadržani tajni podaci

Informacija može da sadrži tajne podatke. Pod tajnim podacima iz stava 1. ovog člana smatraju se podaci koji su u skladu sa propisima o tajnosti podataka prethodno označeni kao tajni.

Ako su u informaciji sadržani tajni podaci, uzbunjivač je dužan da se prvo obrati poslodavcu, a ako se informacija odnosi na lice koje je ovlašćeno da postupa po informaciji, informacija se podnosi rukovodiocu poslodavca.

U slučaju da poslodavac nije u roku od 15 dana postupio po informaciji u kojoj su sadržani tajni podaci, odnosno ako nije odgovorio ili nije preduzeo odgovarajuće

A procedure of internal whistleblowing is initiated by making a disclosure to an employer.

An employer shall act upon the disclosure by which a whistleblowing has been made within 15 days from the day the disclosure was received.

The employer shall inform a whistleblower about the outcome of the procedure upon conclusion thereof, within 15 days after completion of the procedure referred to in paragraph 1 of this Article.

An employer shall, upon a whistleblower's request, provide to him information about the progress of and actions undertaken within the procedure, and enable him to have access to the case file and to participate in actions in the procedure.

Whistleblowing to the Public

The disclosure may be made to the public, without prior disclosure to the employer or authorized authority in the event of imminent threat to life, public health, safety, environment, of large-scale damage, or if there is an immediate risk of evidence being destroyed.

While making a disclosure to the public, a whistleblower shall comply with the presumption of innocence in the court proceedings, right to personal data protection, and shall not jeopardize the conduct of court proceedings.

Whistleblowing when a Disclosure Contains Classified Data

A disclosure may contain confidential data. Classified data referred to in paragraph 1 of this Article are those considered classified in accordance with the regulations on classified data.

If such disclosure contains classified data, a whistleblower shall first address his employer, and if a disclosure refers to a person authorized to act upon disclosures, such disclosure shall be made to the immediate supervisor of that person.

In case that the employer failed to act upon disclosure containing classified information within 15 days or fails to respond or take appropriate measures within his authority,

mere iz svoje nadležnosti, uzbunjivač se može obratiti ovlaštenom organu.

Izuzetno od stava 3. ovog člana, u slučaju da se informacija odnosi na rukovodioca poslodavca, informacija se podnosi ovlaštenom organu.

Ako su u informaciji sadržani tajni podaci, uzbunjivač ne može uzbuniti javnost, ako zakonom nije drugačije određeno.

Ako su u informaciji sadržani tajni podaci, uzbunjivač i druga lica su dužni da se pridržavaju opštih i posebnih mera zaštite tajnih podataka propisanih zakonom koji uređuje tajnost Podataka.

the whistleblower may contact the authorized authority.

Notwithstanding paragraph 3 of this Article, in case a disclosure refers to a manager within the employer, such disclosure shall be made to an authorized authority.

If a disclosure contains classified information, a whistleblower cannot make it public, unless the law provides otherwise.

If a disclosure contains classified information, a whistleblower and other persons shall comply with general and special measures for protection of classified data.

ZAŠTITA UZBUNJIVAČA I NAKNADA ŠTETE

Zabrana stavljanja uzbunjivača u nepovoljniji položaj

Poslodavac ne sme činjenjem ili nečinjenjem da stavi uzbunjivača u nepovoljniji položaj u vezi sa uzbunjivanjem, a naročito ako se nepovoljniji položaj odnosi na:

- 1) zapošljavanje;
- 2) sticanje svojstva pripravnika ili volontera;
- 3) rad van radnog odnosa;
- 4) obrazovanje, osposobljavanje ili stručno usavršavanje;
- 5) napredovanje na poslu, ocenjivanje, sticanje ili gubitak zvanja;
- 6) disciplinske mere i kazne;
- 7) uslove rada;
- 8) prestanak radnog odnosa;
- 9) zaradu i druge naknade iz radnog odnosa;
- 10) učešće u dobiti poslodavca;
- 11) isplatu nagrade i otpremnine;
- 12) raspoređivanje ili premeštaj na drugo radno mesto;
- 13) nepreduzimanje mera radi zaštite zbog uznemiravanja od strane drugih lica;
- 14) upućivanje na obavezne zdravstvene preglede ili upućivanje na preglede radi ocene radne sposobnosti.

Odredbe opšteg akta kojima se uzbunjivaču uskraćuje ili povređuje pravo, odnosno kojima se ova lica stavljaju u nepovoljniji položaj u vezi sa uzbunjivanjem, ništave su.

PROTECTION OF WHISTLEBLOWERS AND COMPENSATION FOR DAMAGE

Prohibition of placing whistleblower in less favorable position

The employer shall not place a whistleblower in a less favorable position related to the whistleblowing by his action or failure to act, especially if the less favorable position relates to:

- 1) employment procedure;
- 2) getting the status of an intern or a volunteer;
- 3) work outside employment;
- 4) education, training and professional development;
- 5) promotion at work, appraisal, acquisition or loss of position;
- 6) disciplinary measures and penalties;
- 7) working conditions;
- 8) termination of employment;
- 9) earnings and other remuneration from employment;
- 10) share in the profits of the employer;
- 11) payment premium and severance pay;
- 12) deployment or transfer to another job;

13) failure to take measures to protect a whistleblower from harassment by others;

14) referral to the mandatory medical examinations or referral to examinations to assess the work capacity.

Provisions of a general act inflicting damaging consequences on a whistleblower

or an associated person due to whistleblowing shall be null and void.

Naknada štete zbog uzbunjivanja

U slučajevima nanošenja štete zbog uzbunjivanja, uzbunjivač ima pravo na naknadu štete, u skladu sa zakonom koji uređuje obligacione odnose.

Sudska zaštita uzbunjivača

Uzbunjivač prema kome je preduzeta štetna radnja u vezi sa uzbunjivanjem ima pravo na sudsku zaštitu.

Sudska zaštita se ostvaruje podnošenjem tužbe za zaštitu u vezi sa uzbunjivanjem nadležnom sudu, u roku od šest meseci od dana saznanja za preduzetu štetnu radnju, odnosno tri godine od dana kada je štetna radnja preduzeta.

U postupku sudske zaštite nadležan je viši sud prema mestu preduzimanja štetne radnje ili prema mestu prebivališta tužioca.

Nadzor nad sprovođenjem zakona

Nadzor nad sprovođenjem ovog zakona vrše inspekcija rada, odnosno upravna inspekcija, u skladu sa zakonima koji uređuju njihova ovlašćenja

U Beogradu

Za Poslodavca / For the Employer:

Richard Wilkinson
direktor / director

Compensation for Damage due to Whistleblowing

In cases of inflicting damaging consequences due to whistleblowing, a whistleblower shall have the right to compensation for damage in accordance with the law regulating contract and torts.

Court Protection due to Whistleblowing

A whistleblower that is likely to suffer damaging consequences due to whistleblowing has the right to court protection.

Court protection is exercised by lodging a lawsuit before a competent court within 6 months from the day of learning about the damaging action undertaken, or 3 years from the day of the occurrence of a damaging consequence.

In the court protection proceedings, the competent court is the higher court in the territory where the damaging action was undertaken or in accordance with the place of adobe of a plaintiff.

Supervision over Enforcement of the Law

Supervision over enforcement of this Law shall be made by the labor inspection, or administrative inspection, in accordance with the laws governing their authorities

In Belgrade

Primljeno dana / Received on

(name of employee)



Annex SLOVAKIA

1 SCOPE

- 1.1 This Annex 1 is prepared in connection to the CTP Group Whistleblower Policy, in order to address any local policies and specific needs, in accordance with the relevant Slovak legislation, concretely the **Act no. 54/2019 Coll. on Protection of Whistleblowers of Anti-social Activity and on Amendments and Supplements to Certain Acts** (the “**Whistleblowers Act**” or “**Legislation**”).
- 1.2 Annex 1 contains provisions that shall be interpreted and applied differently in the Slovak Republic, compared to the provisions of the CTP Group Whistleblower Policy.
- 1.3 Any cases or situations not addressed in Annex 1, shall be governed by the CTP Group Whistleblower Policy.
- 1.4 In the event of any conflict between this Annex 1 and the CTP Group Whistleblower Policy, the provisions of Annex 1 will take precedence.
- 1.5 In the event of any conflict between this Annex 1 and the applicable Legislation, the provisions of the Legislation will take precedence.
- 1.6 This Annex 1 applies to the Slovak entities of the CTP Group in Slovakia, specifically CTP Invest SK, spol. s r.o. and all the individuals subject to it.

2 WHO AND HOW SHOULD I REPORT TO?

Reporting on the Local Level – Slovak Republic

- 2.1 The local whistleblowing channels enable reporting **in writing or orally via hot line**. Upon your request, the report can be made also by means of an **in-person meeting with the Designated Person**, which shall take place within the reasonable timeframe after the request is made.
- 2.2 When reporting through the local whistleblowing channel, you have the following options:
 - **Whistleblowing platform:** more information is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing-slovakia>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).

- **Post mail:** postal item to be sent to the following address: Slovakia, Laurinská 18 811 01 Bratislava-Staré Mesto, to the attention of the respective Designated Person (**do not forget to include the name of the Designated Person on the envelope!**)
- **Hot line:** the phone number for the hotline for individual CTP Group entities is available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing-slovakia>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).
- **In-person meeting:** please, contact the Designated Person for your CTP Group entity.
- **E-mail to the Designated Persons:** use the email address specifically designated for receiving whistleblowing reports, available on the intranet (<https://intranet.ctp.eu/web/guest/whistleblowing-slovakia>) or website (<https://ctp.eu/ctp-policies/how-to-report-a-concern/>).

2.3 Should there be a conflict of interest between the Designated Person and the person being verified or the report being verified (or if there is even a potential conflict of interest), the Whistleblower shall use alternative channels to report, as stipulated in paragraph 4.6 to 4.10 of the CTP Group Whistleblower Policy. In such case, the CTP Group Whistleblower Policy shall cover the procedure, and its provisions shall be applied.

3 WHAT IF I WILL NOT BE SATISFIED WITH THE RESULT OF THE VERIFICATION?

3.1 The result of the verification of the report will also include information for the Whistleblower, to which authorities can the Whistleblower turn in case of non-satisfaction with the result of the verification, and that there is also the option submit the report to the law enforcement authorities.

4 RECORD OF REPORTS

4.1 The CTP Group Entity is obliged to keep records of reports within 3 years from the date of delivery of the report to the extent of:

- a) the date of delivery of the report,
- b) name, surname and residence of the Whistleblower; unless an anonymous Whistleblower,
- c) subject of the report,
- d) the result of verifying the report,
- e) date of completion of the report verification.

4.2 The records of reports shall be separated from any other internal records, are safely locked and only employees carrying out the duties of the Designated Person shall have access to it.

5 WHICH CONCERNS ARE COVERED BY THIS POLICY?

5.1 Complementary to point 3.3. in the CTP Group Whistleblower Policy, as a serious anti-social activity shall be considered also:

- the following crimes according to the Slovak Criminal Code⁶: § 168, § 170, § 170b, § 177, § 212, § 213, § 217, § 221, § 226, § 233a, § 237 to 240, § 243, § 243a, § 247, § 247d, § 251a, § 252 to 254, § 261 to 263, § 266 to 268, § 271, § 278a, § 283, § 299a, § 302, § 305, § 326 to 327a, § 328 to 336b, § 336d, § 348, § 352a or § 374;
- crime for which the Criminal Code provides a prison sentence with a maximum penalty exceeding 2 years;
- an administrative offense for which a fine with an upper limit determined by calculation can be imposed, or
- an administrative offense for which a fine with an upper limit of at least EUR 30.000 can be imposed.

6 HOW WILL I BE PROTECTED AGAINST RETALIATION IF I REPORT A CONCERN?

- 6.1 According to the Slovak legislation, no Whistleblower shall waive the right to protection from retaliation.

7 CAN I ASK SOMEONE FOR ADVICE?

- 7.1 The Slovak Office for the Protection of Whistleblowers provides advice and consultations in connection with the reporting of anti-social activity. Whistleblowers can contact the office on the free helpline 0800 221 213.

8 INFORMATION ON THE EXTERNAL WHISTLEBLOWING CHANNELS

- 8.1 Based on the Slovak law, Whistleblowers shall be able to seek protection and report Breaches through the following external whistleblowing channels:
- **Office for the Protection of Whistleblowers**
 - Electronically: <https://formular.oznamovatelia.sk/form/mail>
 - By mail/personally at: Námestie slobody 29, 811 06 Bratislava
 - **Prosecutor's Office**
 - For more information visit: <https://www.genpro.gov.sk/en/index/>
 - **Any administrative authority to which your complaint relates and may impose a fine**
 - for example, the Central Labor Office: antikorupcia@upsvr.gov.sk

9 FINAL PROVISIONS

- 9.1 CTP Group hereby undertakes to train and educate the Designated Person, managers and employees regarding the agenda of whistleblowing.

⁶ Act no. 300/2005 Coll. Criminal Code



Annex Poland



Separate Policy follows.



**PROCEDURA ZGŁOSZEŃ
WEWNĘTRZNYCH /
INTERNAL REPORTING PROCEDURE**

CTP INVEST POLAND SP. Z O. O.

Warszawa, 1 października 2024 r.

**PROCEDURA ZGŁOSZEŃ
WEWNĘTRZNYCH
CTP INVEST POLAND SP. Z O.O.
(„Procedura”)**

**INTERNAL REPORTING
PROCEDURE
AT CTP INVEST POLAND SP. Z O.O.
("Procedure")**

Jaki jest cel wdrożenia Procedury?

W CTP Invest Poland Sp. z o.o.(„**Spółka**”) w prowadzeniu biznesu kierujemy się najwyższymi standardami przestrzegania przepisów prawa, zasad compliance oraz etyki.

Wdrażamy Procedurę, aby każdy mógł skorzystać z przygotowanych kanałów zgłoszeń i poinformować nas o dostrzeżonych nieprawidłowościach lub zachowaniach, które są sprzeczne z wartościami Spółki.

Każda z osób, która dokona stosownego zgłoszenia otrzyma od Spółki pełne wsparcie oraz ochronę przed działaniami odwetowymi.

Jakie nieprawidłowości należy zgłaszać?

Chcemy wiedzieć o wszelkich działaniach lub zaniechaniach niezgodnych z prawem lub mających na celu obejście prawa, które dotyczą Spółki („**Naruszenie**”). Dzięki Twojemu zgłoszeniu będziemy w stanie je szybciej zidentyfikować i wyeliminować.

Podstawowy katalog naruszeń prawa, który warto nam zgłaszać obejmuje w szczególności następujące obszary:

- korupcja;
- ochrona środowiska;
- ochrona prywatności i danych osobowych;
- bezpieczeństwo sieci i systemów teleinformatycznych;

What is the purpose of implementing the Procedure?

At CTP Invest Poland Sp. z o.o. (“**Company**”), we are guided by the highest standards of legal compliance, compliance rules and ethics in conducting business.

We are implementing the Procedure so that everyone can use the prepared reporting channels and inform us of perceived irregularities or behavior that goes against the Company's values.

Any person who makes an appropriate report will receive full support and protection from retaliation from the Company.

What irregularities should be reported?

We want to know about any illegal acts or omissions or those intended to circumvent the law that involve the Company (“**Violation**”). With your report, we will be able to identify and eliminate them more quickly.

The basic catalog of legal violations worth reporting to us includes in particular the following areas:

- corruption;
- environmental protection;
- protection of privacy and personal data;
- security of networks and ICT systems;

- przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu;
- bezpieczeństwo transportu;
- konflikt interesów;
- bezpieczeństwo i higiena pracy;
- nieprawidłowe korzystanie z zasobów Spółki;
- jakiegokolwiek formy dyskryminacji, w tym molestowania i mobbingu;
- wewnętrzne procedury obowiązujące w Spółce, w szczególności Procedury antymobbingowej;
- counteracting money laundering and terrorist financing;
- transport safety;
- conflict of interests;
- OHS;
- improper use of the Company's resources;
- any kind of discrimination, including harassment and mobbing;
- internal procedures applicable to the Company, in particular the Anti-harrassment Procedure;

Zachęcamy Was do dokonywania zgłoszeń w ramach zakresu wskazanego w ustawie o ochronie sygnalistów, oraz powyżej wyróżnionych kwestii.

We encourage you to make reports within the scope indicated in the Whistleblower Protection Act, and also on the issues highlighted above.

Jeśli masz wątpliwości czy Twoje zgłoszenie mieści się w powyższym katalogu, dokonaj zgłoszenia, a my zajmiemy się resztą.

If you have doubts about whether your report falls within the above catalog, make the report and we will take care of the rest.

Kto może dokonywać zgłoszeń?

Who can make a report?

Zachęcamy, aby każdy kto ma wiedzę o Naruszeniu skorzystał z Procedury i dokonał zgłoszenia.

We encourage anyone with knowledge of the Violation to use the Procedure and make a report.

Procedura dedykowana jest w szczególności pracownikom, współpracownikom, kandydatom, stażystom, dostawcom czy kontrahentom Spółki.

The procedure is dedicated in particular to employees, associates, candidates, trainees, suppliers or contractors of the Company.

Sygnalistą w rozumieniu Procedury jest osoba fizyczna, która w ramach Procedury zgłasza informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą, niezależnie od podstawy prawnej (lub jej braku) łączącej tę osobę ze Spółką.

A Whistleblower within the meaning of this Procedure is a natural person who, as part of the Procedure, reports information about a breach of law obtained in a work-related context, regardless of the legal basis (or lack thereof) between that person and the Company.

Sygnalista podlega ochronie wynikającej z ustawy o ochronie sygnalistów od chwili dokonania zgłoszenia, pod warunkiem że

A whistleblower is subject to the protection of the Whistleblower Protection Act from the moment he or she makes a report, provided

miał uzasadnione podstawy sądzić, że informacja będąca przedmiotem zgłoszenia jest prawdziwa w momencie jego dokonywania i że stanowi informację o naruszeniu prawa.

that he or she had reasonable grounds to believe that the information that is the subject of the report was true at the time it was made and that it constitutes information about a violation of the law.

Za Sygnalistę nie będzie uważana osoba, która dokonuje zgłoszenia w złej wierze, czyli wtedy, kiedy dokonuje świadomego zgłoszenia nieprawdziwej informacji, a także gdy dokonuje tego w innym celu niż poinformowanie Spółki o mających miejsce lub mogących wystąpić nieprawidłowościach.

A person who makes a report in bad faith, i.e. when he or she knowingly reports false information, and when he or she does so for a purpose other than to inform the Company of irregularities that are taking place or that may occur, will not be considered a Whistleblower.

Czy można dokonać zgłoszenia anonimowo?

Can a report be made anonymously?

Spółka dopuszcza dokonywanie zgłoszeń anonimowych. Zgłoszenie nie musi zawierać danych, które bezpośrednio lub pośrednio pozwalają na zidentyfikowanie Waszej tożsamości, jak również danych umożliwiających kontakt zwrotny do Was.

The Company allows anonymous reporting. The report does not have to contain data that directly or indirectly allows your identification, as well as data that allows you to be contacted back by the Company.

Ze względu na ochronę przysługującą osobie zgłaszającej Naruszenie, zachęcamy jednak do ujawniania swojej tożsamości i dokonywania zgłoszenia nieanonimowo. Decyzja co do dokonania zgłoszenia anonimowo lub z podaniem danych umożliwiających zidentyfikowanie tożsamości należy jednak wyłącznie do Was.

However, due to the protections afforded to the person reporting the Violation, we encourage you to disclose your identity and make your report anonymously. However, the decision as to whether to report anonymously or with personally identifiable information is entirely up to you.

Z jakich kanałów zgłoszeń można skorzystać w Spółce?

What report channels can be used within the Company?

Zgłoszeń możecie dokonywać ustnie lub pisemnie za pomocą dedykowanych kanałów dostępnych w Spółce.

You can make reports orally or in writing through the dedicated reporting channels available within the Company.

Zgłoszenia ustne mogą być dokonywane:

Oral reports can be made:

- osobiście – poprzez spotkanie w godzinach we wcześniej umówionym terminie (nie później niż w ciągu 7 dni od przekazania takiego wniosku przez Sygnalistę).
- in person - by meeting in hours on a pre-arranged date (no later than 7 days after the Whistleblower has forwarded such a request).

Zgłoszenia pisemne mogą być dokonywane:

- w postaci papierowej – korespondencja powinna być kierowana na adres Spółki z dopiskiem „Poufne – Sygnalista”;
- elektronicznie – na adres e-mail whistleblowingPL@ctp.eu.

Reports in writing can be made:

- in paper form – correspondence should be addressed to the Company's address with the notation “Confidential - Whistleblower”;
- electronically – to the email address whistleblowingPL@ctp.eu.

Spółka umożliwia Wam również przekazanie informacji o Naruszeniach innymi kanałami, na odrębnie określonych zasadach. Spółka należy do grupy kapitałowej CTP, gdzie jest już grupowy system zgłaszania nieprawidłowości. Skorzystanie z systemu zgłaszania nieprawidłowości poprzez grupowy kanał zgłoszeń skutkuje tym, że Wasze zgłoszenie będzie rozpoznawane na zasadach określonych w grupowym systemie zgłaszania nieprawidłowości. Skorzystanie z systemu zgłaszania nieprawidłowości na poziomie grupy nie wyłącza Waszej ochrony wynikającej z ustawy o ochronie sygnalistów. W razie pytań dotyczących zgłoszeń poprzez grupowy system zgłaszania nieprawidłowości prosimy o kontakt z działem HR.

The Company also allows you to provide information on Violations through other channels, under separately defined rules. The Company operates as a part of CTP capital group, where a whistleblowing system is already in place. Using the group whistleblowing system will result in your report being recognized under the terms of the group – whistleblowing system. Using the group – level whistleblowing system does not exclude your protection under the Whistleblowing Protection Act. In case of any questions regarding the group – level whistleblowing system please address to the HR.

W ramach grupowego systemu zgłaszania nieprawidłowości możecie dokonać zgłoszeń ustnie lub pisemnie za pomocą dedykowanych kanałów dostępnych na poziomie grupy.

Under the group – level whistleblowing system you can make reports orally or in writing through the dedicated reporting channels available within the group.

Szczegółowe informacje znajdują się w Intranecie w zakładce Whistleblowing.

More detailed information can be found on the Intranet in the Whistleblowing tab.

Jakie są zasady dokonywania zgłoszeń?

Wasze zgłoszenie powinno zawierać przejrzyste i możliwie pełne wyjaśnienie na czym polega Naruszenie.

Zachęcamy, abyście w zgłoszeniu opisywali tło danej sytuacji, wskazywali kiedy miała ona miejsce i na czym polegało nieprawidłowe działanie, a także przedstawiali jak najwięcej dodatkowych informacji, takich jak listę świadków czy posiadane przez Was dowody (e-maile, fotografie, zestawienia, faktury, itp.).

Przy składaniu zgłoszenia rekomendujemy, abyście podawali adres do kontaktu (np. adres korespondencyjny, adres e-mail czy choćby numer telefonu). Brak jego przekazania uniemożliwi lub znacznie utrudni komunikację pomiędzy nami, a w konsekwencji może uniemożliwić przekazanie Wam potwierdzenia przyjęcia zgłoszenia lub informacji zwrotnej po zakończeniu działań następczych.

Kto przyjmuje i rozpatruje zgłoszenia?

Osobą upoważnioną przez Spółkę do przyjmowania Waszych zgłoszeń jest **HR Manager** pełniący funkcję Wyjaśniającego.

Jednostką upoważnioną do rozpatrywania zgłoszeń (podejmowania działań następczych) jest komisja wyjaśniająca („**Komisja**”). W skład Komisji wchodzić będą: Head of Legal Department, osoba z działu HR oraz przedstawiciel osób zatrudnionych. Wszyscy członkowie Komisji każdorazowo otrzymają od Spółki stosowne upoważnienia do rozpatrywania zgłoszeń.

Przedstawiciel osób zatrudnionych będzie każdorazowo wybierany przez pozostałych

What are the rules for reporting?

Your report should include a clear and as complete as possible explanation of what the Violation consists of.

We encourage you to describe the background of the situation in your report, indicate when it occurred and what the malfunction consisted of, and provide as much additional information as possible, such as a list of witnesses or evidence you have (emails, photographs, statements, invoices, etc.).

When submitting a request, we recommend that you provide a contact address (e.g., mailing address, e-mail address or even a telephone number). Failure to provide it will make communication between us impossible or significantly more difficult, and as a result, we may not be able to provide you with an acknowledgement or feedback after follow-up actions.

Who accepts and processes reports?

The person authorized by the Company to receive your reports and subsequently handle them (follow – up actions) is **HR Manager**, acting as the Explainer.

The entity authorized to handle (follow-up actions) is explanatory committee (“**Commission**”). The Commission will consist of: Head of Legal Department, member of the HR Department, and workers’ representative. All members of the Commission will receive appropriate authorizations from the Company to consider applications in each case.

The workers’ representative will be selected each time by the other members of the

członków Komisji poprzez losowanie, z zastrzeżeniem, że przedstawiciel nie może być członkiem Zarządu lub z tego samego zespołu, co osoba zgłaszająca naruszenie. W przypadku, kiedy wylosowany przedstawiciel nie zgodzi się na udział w Komisji, odbędzie się losowanie kolejnej osoby.

W uzasadnionych okolicznościach w skład Komisji mogą zostać powołani eksperci zewnętrzni, w tym szczególności doradcy prawni czy Group AML Compliance Officer.

W uzasadnionych okolicznościach, np. w przypadku konfliktu interesów czy długotrwałej nieobecności Wyjaśniającego, Spółka może pisemnie upoważnić inną osobę do przyjmowania zgłoszeń.

Przed dokonaniem zgłoszenia macie możliwość nieformalnego skonsultowania Waszych wątpliwości dotyczących ewentualnego Naruszenia z Wyjaśniającym lub Waszym bezpośrednim przełożonym. Odbycie konsultacji nie jest równoznaczne z dokonaniem zgłoszenia Naruszenia. Konsultacje odbywają się na zasadach poufności i nie stanowią bezpośredniej podstawy do podjęcia działań następczych.

Jeżeli zgłoszenie dotyczy jednego z członków Komisji, zgłoszenie będzie rozpatrzone przez dwuosobowy skład Komisji z wyłączeniem członka, którego dotyczy zgłoszenie.

W uzasadnionych okolicznościach w skład Komisji mogą zostać powołani eksperci zewnętrzni, w tym szczególności doradcy prawni czy Group AML Compliance Officer.

Jeżeli Wasze zgłoszenie dotyczy Naruszenia na poziomie struktury grupy lub dotyczy

Commission by drawing lots, with the proviso that the representative cannot be a member of the Management Board or from the same team as the person reporting the violation. In the event that the representative selected does not agree to participate in the Commission, the next person will be drawn.

Under reasonable circumstances, external experts, including in particular legal advisers or Group AML Compliance Officer may be appointed to the Commission.

Under reasonable circumstances, such as a conflict of interest or the long-term absence of the Explainer, the Company may authorize another person in writing to receive reports.

Before making a report, you have the opportunity to informally consult your concerns about a possible Violation with the Explainer or your immediate supervisor. Holding a consultation is not equivalent to making a report of a Violation. Consultations are held on a confidential basis and are not a direct ground for follow-up action.

If the report concerns one of the members of the Commission, the report will be handled by two members of the Commission excluding the member concerned.

Under reasonable circumstances, external experts, including in particular legal advisers or Group AML Compliance Officer may be appointed to the Commission.

If your report concerns a Violation at the global level, or concerns a Violation in two or

Naruszenia w dwóch lub więcej podmiotach powiązanych, a po dokonaniu weryfikacji zgłoszenie nie będzie mogło zostać skutecznie rozpatrzone na zasadach przewidzianych Procedurą, Wyjaśniający poinformuje Was o tym, jednocześnie wskazując, że Wasze zgłoszenie będzie mogło zostać przekazane do Group AML Compliance Officer, celem jego skutecznego rozpatrzenia. Przekazanie zgłoszenia odbywa się z zachowaniem wszelkich zasad dotyczących poufności określonych Procedurą. Przekazanie zgłoszenia może być dokonane wyłącznie za Waszą zgodą.

Jeśli nie wyrazicie zgody na przekazanie zgłoszenia, rozpatrzemy je lokalnie w zakresie, w jakim będziemy mieć taką możliwość.

Po otrzymaniu informacji o tym, że Wasze zgłoszenie nie będzie mogło zostać skutecznie rozpatrzone na zasadach przewidzianych Procedurą macie możliwość wycofania zgłoszenia. Będzie to skutkowało brakiem podjęcia przez nas żadnych działań następczych.

Jakie działania następcze podejmuje Spółka?

Jeśli Wasze zgłoszenie spełni wymogi określone w Procedurze, Spółka ma obowiązek podjęcia, z zachowaniem należytej staranności, działań następczych w celu oceny prawdziwości informacji o Naruszeniu, a w stosownych przypadkach w celu przeciwdziałania Naruszeniu lub jego skutkom.

Każdorazowo po wpłynięciu zgłoszenia nieprawidłowości, Wyjaśniający dokonuje niezwłocznie jego wstępnej analizy, a następnie o ile jest to możliwe, Wyjaśniający potwierdzi Wam w terminie nie

more affiliated entities, and after analysis of the report cannot be successfully processed under the rules of the Procedure, the Explainer will inform you of this, while indicating that your report can be transferred to Group AML Compliance Officer to process it effectively. The transfer of your report shall be made in compliance with all confidentiality rules set forth in the Procedure. The transfer of the report can be made only with your consent.

If you do not agree to forward your report, we will process it locally to the extent that we have the ability to do so.

Once you have been informed that your report will not be able to be successfully processed under the terms of the Procedure, you have the option to withdraw your report. This will result in no follow-up actions taken by us.

What follow-up actions is the Company taking?

If your report meets the requirements set forth in the Procedure, the Company has an obligation to follow up with due diligence to assess the veracity of the information about the Violation and, if applicable, to prevent the Violation or its consequences.

Whenever a report is received, the Explainer will immediately perform a preliminary analysis of the report, and then, if possible, the Explainer will confirm to you within no more than 7 days the acceptance of the

dłuższym niż 7 dni przyjęcie zgłoszenia, chyba że nie podacie danych kontaktowych, na które należy przekazać potwierdzenie. Potwierdzenie przyjęcia zgłoszenia anonimowego nie prowadzi do ujawnienia Waszej tożsamości.

Wyjaśniający przekazuje Wam informację zwrotną o rozpatrzeniu zgłoszenia i działaniach następczych – nie później niż po upływie 3 miesięcy od potwierdzenia przyjęcia zgłoszenia, chyba że nie podacie adresu do kontaktu, na który należy przekazać Wam informację zwrotną i nie jest to technicznie możliwe bez tego wskazania. Informacja zwrotna obejmuje m.in. informację o stwierdzeniu bądź braku stwierdzenia wystąpienia naruszenia prawa, i ewentualnych środkach, które zostały lub zostaną zastosowane w reakcji na stwierdzone naruszenie prawa.

Na czym polega zakaz działań odwetowych?

Jako działanie odwetowe rozumieć należy jakiegokolwiek, bezpośrednie lub pośrednie, działanie lub zaniechanie w kontekście związanym z pracą, które jest spowodowane dokonaniem przez Was zgłoszenia i które narusza lub może naruszyć Wasze prawa lub wyrządza lub może wyrządzić Wam nieuzasadnioną szkodę. Zakaz działań odwetowych obejmuje także osoby pomagające Wam w dokonaniu zgłoszenia oraz osoby z Wami powiązane.

Dokonanie zgłoszenia nie oznacza przyznania Wam immunitetu za jakiegokolwiek naruszenie, w które mogliście być zaangażowani. Zgłoszenie nie wyklucza m.in. możliwości rozwiązania z Wami umowy o pracę lub innego stosunku prawnego będącego podstawą zatrudnienia w Spółce w przypadkach i na zasadach

report, unless you do not provide contact information to which the confirmation should be forwarded. Confirmation of acceptance of an anonymous report does not lead to disclosure of your identity.

The Explainer shall provide you with feedback on the consideration of the report and follow-up - no later than 3 months after the acknowledgment of the report, unless you do not provide a contact address to which the feedback should be provided to you and it is not technically possible without this indication. The feedback shall include, among other things, information on whether or not a violation of the law has been established, and what measures, if any, have been or will be taken in response to the established violation of the law.

What is a prohibition on a retaliation?

Retaliation shall be understood as any act, direct or indirect, in a work-related context that is caused by your report and that violates or may violate your rights or causes or is likely to cause unjustified harm to you. The prohibition on retaliation also extends to those who assisted you in making the report and those associated with you.

Making a report does not confer immunity for you for any violation in which you may have been involved. Report does not preclude, among other things, the possibility of terminating your employment contract or other legal relationship that is the basis of your employment with the Company in cases and in accordance with the law, for example

zgodnych z przepisami prawa, przykładowo, kiedy uczestniczyliście w zgłoszonym naruszeniu prawa.

in case you participated in the reported violation.

Ochrona przewidziana w Procedurze nie ma zastosowania w przypadku zgłoszenia dokonanego w złej wierze.

The protection provided for in the Procedure does not apply in the case of a report made in bad faith.

Pamiętajcie, że niezależnie od dokonania zgłoszenia, pozostajecie zobowiązani wykonywać swoją pracę i obowiązki zawodowe sumiennie i starannie oraz stosować się do poleceń Spółki, które dotyczą pracy.

Regardless of whether the report is made, the Whistleblower remains obliged to perform his/her work and professional duties conscientiously and diligently and to comply with the Company's instructions regarding the work.

Szczegółowe uregulowania w zakresie ochrony znajdują się w Rozdziale 2 ustawy o ochronie sygnalistów.

The detailed protection regulations are found in Chapter 2 of the Whistleblower Protection Act.

Jak dbamy o zachowanie poufności?

How we ensure confidentiality?

Tożsamość Sygnalisty, jak również wszystkie informacje umożliwiające jego identyfikację, są traktowane jako tajemnica Spółki na wszystkich etapach procesu rozpatrywania zgłoszonych nieprawidłowości.

The identity of the Whistleblower, as well as all information enabling their identification, are treated as a secret of the Company at all stages of the process of handling the reported irregularities. In particular, the identity of the Whistleblower will not be disclosed to the entities affected by the irregularity report, third parties or other employees and associates of the Company, unless it results from generally applicable laws in the context of ongoing investigations by relevant authorities. We take an analogous approach to the confidentiality of the identity of the persons assisting the Whistleblower or the persons affected by the report.

W szczególności tożsamość Sygnalisty nie będzie ujawniana osobom, których dotyczy zgłoszenie nieprawidłowości, osobom trzecim ani innym pracownikom i współpracownikom Spółki, chyba że wynika to z powszechnie obowiązujących przepisów prawa w kontekście prowadzonych postępowań przez stosowne organy. Analogicznie podchodzimy do poufności tożsamości osób pomagających Sygnaliście czy osób, których zgłoszenie dotyczy.

Czy można dokonywać zgłoszeń poza Spółką?

Can a report be made outside the Company?

Każdy z Was ma możliwość dokonania zgłoszenia bezpośrednio do Rzecznika Praw Obywatelskich albo organów publicznych

Each of you can report directly to the Ombudsman or to public authorities and - where applicable - to the institutions, bodies,

oraz – w stosownych przypadkach – do instytucji, organów lub jednostek organizacyjnych Unii Europejskiej („Zgłoszenie zewnętrzne”). Zgłoszenia zewnętrzne mogą być dokonane według odpowiednich procedur obowiązujących w danym organie.

Zachęcamy Was jednak, aby wszelkie zgłoszenia w zakresie spraw określonych w Procedurze były kierowane w pierwszej kolejności do nas na zasadach określonych w Procedurze. Pozwoli to nam na podjęcie natychmiastowych działań.

O czym jeszcze warto pamiętać?

Wszelkie utrudnianie dokonywania zgłoszenia lub uniemożliwianie tego, w szczególności przy zastosowaniu przemocy, gróźb lub podstępu, a także podejmowanie działań odwetowych może skutkować pociągnięciem do odpowiedzialności, w tym nawet do rozwiązania stosunku pracy bez wypowiedzenia z winy takiego pracownika.

Procedurę przekazujemy Wam zarówno poprzez pocztę elektroniczną, jak i umieszczamy na tablicach ogłoszeń. Procedura jest również dostępna w Dziale HR na każde Wasze żądanie.

Procedura została skonsultowana z Przedstawicielami osób świadczących pracę na rzecz Spółki.

W wypadku rozbieżności pomiędzy polską i angielską wersją językową Procedury, rozstrzygające znaczenia ma wersja polska.

Wszelkie pytania dotyczące Procedury i zgłaszania nieprawidłowości kierujcie do działu HR.

offices or agencies of the European Union ("**External Report**"). External reports can be made according to the relevant procedures of the authority.

However, we encourage you that all reports regarding matters specified in the Procedure should be addressed to us in the first place on the terms set out in this Procedure. This will allow us to take immediate action.

What else is worth remembering?

Any obstruction or prevention from making a report, in particular by the use of violence, threats or deception and taking retaliatory actions may result in liability, including even termination of employment without notice due to the fault of such an employee.

The Procedure is communicated to you both via email and posted on the notice boards. The Procedure is also available in the HR Department whenever you request it.

The procedure has been consulted with Representatives of persons providing work for the Company.

In the event of any discrepancy between the Polish and the English language version of the Procedure, the Polish version shall prevail

Any questions regarding the procedure and irregularities reports you can direct to the HR Department.

Załącznik:

1) Suplement klauzuli informacyjnej dot. danych osobowych przetwarzanych przez CTP Invest Poland Sp. z o.o.

Appendix:

1) Information clause supplement on the processing of personal data by CTP Invest Poland Sp. z o.o.

Podpisano 1 października 2024 roku.

Spółka / Company

Dominika Duda-Słoma

Piotr Flugel

**Przedstawiciele osób świadczących pracę na rzecz Spółki: /
The Representatives of persons providing work for the Company:**

*Potwierdzamy, że Procedura została z nami skonsultowana.
We confirm that the Procedure was consulted with us.*

Paweł Błaszczak

Mateusz Grabarczyk

Małgorzata Kuplińska

Załącznik numer 1

Suplement klauzuli informacyjnej dot. danych osobowych przetwarzanych przez CTP Invest Poland Sp. z o.o.

Ogólna klauzula danych osobowych jest dostępna tutaj: <https://ctp.eu/pl/polityka-ctp/zgoda-na-przetwarzanie-danych-osobowych/>

- Pani/Pana dane osobowe przetwarzane będą wyłącznie w związku z przyjmowaniem i weryfikacją zgłoszeń wewnętrznych oraz podejmowaniem działań następczych w celu wypełnienia obowiązku prawnego ciążącego na Spółce jako administratorze tj. w celu przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego.
- W przypadku gdy dane osobowe pozyskiwane są od osoby, której dane dotyczą, podanie danych osobowych jest dobrowolne.
- Podstawą prawną przetwarzania Pani/Pana danych osobowych będzie wypełnianie obowiązków prawnych ciążących na Spółce jako administratorze (art. 6 ust. 1 lit. c RODO), w zakresie danych szczególnej kategorii (art. 9 ust. 2 lit. g RODO). Dane osobowe gromadzone w rejestrze zgłoszeń wewnętrznych są przetwarzane w celu realizacji obowiązku prawnego ciążącego na Spółce (art. 6 ust.1 lic c RODO w zw. z art. 29 ust. 1 Ustawy z dnia 14 czerwca 2024r. o ochronie sygnalistów (Dz.U. 2024 poz. 928).
- Odbiorcami Pani/Pana danych osobowych mogą być organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z

Appendix no. 1

Information clause supplement on the processing of personal data by CTP Invest Poland Sp. z o.o.

The general personal data clause is available here: <https://ctp.eu/pl/polityka-ctp/zgoda-na-przetwarzanie-danych-osobowych/>

- Your personal data will only be processed for the purposes related to receiving and verifying reports and taking follow – up actions in order to fulfillment of legal obligations of the Company as a controller i.e. to receive or take possible follow – up action.
- In event where personal data is obtained from the data subject, the provision of personal data is voluntary.
- The legal basis for the processing of your personal data will be the fulfillment of legal obligations of the Company as a controller (Article 6(1)(c) GDPR), regarding special category data (Article 6(2)(g) GDPR). Personal data collected in the register of internal reports is processed for the purpose of fulfilling the Company's legal obligation (Article 6 (1)(c) GPDR) in conjunction with Article 29 (1) of the Act of June 14th 2024 on the Protection of Whistleblowers (Dz.U. 2024 poz. 928)
- The recipients of your personal data may be public authorities and entities performing public tasks or acting on behalf of public authorities, to the extent and for the purposes set out by the applicable law, and entities to which the

przepisów prawa oraz podmioty, którym Spółka zleca wykonywanie czynności, z którymi wiąże się przetwarzanie danych osobowych. Dane osobowe mogą być ujawnione podmiotowi upoważnionemu przez Spółkę do przyjmowania zgłoszeń wewnętrznych oraz podmiotom świadczącym usługi doradztwa prawnego.

- Dane osobowe są przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze lub po zakończeniu postępowań zainicjowanych tymi działaniami, a w przypadku gdy odmówiono przyjęcia zgłoszenia – przez okres 3 lat po zakończeniu roku kalendarzowego, w którym odmówiono przyjęcia zgłoszenia, chyba że dokumenty związane ze zgłoszeniem stanowią część akt postępowań przygotowawczych lub spraw sądowych lub sądownoadministracyjnych. W takim przypadku dane osobowe będą przechowywane do czasu prawomocnego zakończenia właściwego postępowania. Nie dotyczy to danych osobowych zgromadzonych w dokumentach roboczych wytworzonych wyłącznie w celu usprawnienia postępowania, które są przechowywane do momentu zakończenia postępowania wyjaśniającego.
- Pani/Pana dane osobowe nie są przekazywane do państwa trzeciego lub organizacji międzynarodowej.
- Posiada Pani/Pan prawo dostępu do treści swoich danych i ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych, oraz prawo do cofnięcia zgody, jeśli jest ona podstawą przetwarzania Pani/Pana danych osobowych, przy czym cofnięcie zgody nie ma wpływu na zgodność z

Company outsources the processing of personal data. Personal data may be disclosed to the entity authorized by the Company to receive internal reports and to entities providing legal advising services.

- Personal data shall be retained for a period of 3 years after the end of the calendar year in which the follow-up actions were completed or after the completion of the proceedings initiated by these actions, and in the case of a denied notification - for a period of 3 years after the end of the calendar year in which the notification was denied, unless the documents related to the notification are part of the files of pre-trial proceedings or court or judicial-administrative cases. In this case, personal data will be kept until the relevant proceedings are legally concluded. This does not apply to personal data collected in working documents produced for the sole purpose of facilitating the proceedings, which are kept until the investigation is completed.
- Your personal data are not transferred to third country or international organization.
- You have the right to access and rectify, delete or restrict the processing of your personal data, the right to object to the processing, as well as the right to data portability, and the right to withdraw consent for the processing of your personal data if it was the basis for the processing; however, consent withdrawal does not affect the lawfulness of data

prawem przetwarzania danych, które było dokonywane na podstawie zgody przed jej wycofaniem;

processing carried out based on such consent before its withdrawal;

- Podane dane będą przetwarzane na podstawie Ustawy z dnia 14 czerwca 2024r. o ochronie sygnalistów (Dz.U. 2024 poz. 928) oraz zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych; RODO);
 - W przypadku gdy dane osobowe nie zostały pozyskane od osoby, której dane dotyczą, administrator nie podaje tej osobie informacji o których mowa w art. 14 ust. 1 i 2 RODO w sytuacjach o których mowa w art. 14 ust. 5 RODO (m.in. gdy udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku). Inspektor nie podaje informacji o źródle pochodzenia danych osobowych oraz nie przekazuje tej informacji w trybie art. 15 ust. 1 lit. g RODO, chyba że Sygnalista nie spełnia warunków wskazanych w art. 6 ustawy o ochronie sygnalistów albo wyraził wyraźną zgodę na ujawnienie swojej tożsamości.
 - Ma Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy Ogólnego rozporządzenia o ochronie danych.
- The provided data will be processed according to the Act of June 14th 2024 on the Protection of Whistleblowers (Dz.U. 2024 poz. 928) and in compliance with the 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; GDPR);
 - Where personal data has not been obtained from the data subject, the administrator shall not provide that person with the information referred to in Article 14(1) and (2) of the RODO in situations referred to in Article 14(5) of the RODO (among other things, where providing such information proves impossible or would require disproportionate effort). The Inspector shall not provide information about the source of personal data and shall not provide this information pursuant to Article 15(1)(g) RODO, unless the Whistleblower does not meet the conditions indicated in Article 6 of the Act on the Protection of Whistleblowers, or has expressly consented to the disclosure of his or her identity.
 - If you believe that the processing of your personal data violates the provisions of the General Data Protection Regulation, You have the right to lodge a complaint with the President of the Personal Data Protection Office.