

	INTERNAL PROCEDURE FOR REPORTING BREACHES OF LAW AND OTHER VIOLATIONS, TAKING FOLLOW-UP ACTION, AND SETTING OUT THE CONDITIONS FOR PROTECTING PERSONS REPORTING BREACHES, IN FORCE AT RAINBOW TOURS S.A.	
Legal basis for issuance:	Article 25 of the Act of 14.06.2024 on the Protection of Whistleblowers (Journal of Laws of 2024, item 928), implementing into Polish law Directive (EU) 2019/1937 of the European Parliament and of the Council of 23.10.2019 on the protection of persons who report breaches of Union law (OJ EU L 305 of 26.11.2019, p. 17, and OJ EU L 347 of 20.10.2020, p. 1) Article 97d of the Act of 29.07.2005 on Public Offering and the Conditions for Introducing Financial Instruments to an Organized Trading System, and on Public Companies (i.e. Journal of Laws of 2020, item 2080, as amended)	
Internal or resolution number:	Management Board: Resolution No. 02/01/20 of 17.01.2020; Resolution No. 02/09/24 of 17.09.2024	Supervisory Board: not applicable
Distribution list:	All organizational units of Rainbow Tours S.A., companies of the Rainbow Tours Capital Group	
Effective from / management review:	25.09.2024	not applicable / ongoing
Document owner:	Management Board	
Internal normative acts amended / repealed:	"Anti-Corruption Policy of the Rainbow Tours Capital Group," adopted by Management Board Resolution No. 02/12/17 of 21.12.2017 [Appendix No. 5 to the referenced resolution] — amendment concerning the "Whistleblowing Procedure"	
Related internal normative acts:	"Anti-Corruption Policy of the Rainbow Tours Capital Group," adopted by Management Board Resolution No. 02/12/17 of 21.12.2017 [Appendix No. 5 to the referenced resolution]	
Attachments:	Not applicable	

I. GENERAL PROVISIONS	2
II. SCOPE OF THE PROCEDURE	6
III. REPORTING BREACHES; RULES FOR NOTIFYING BREACHES	8
IV. PRELIMINARY ANALYSIS AND VERIFICATION OF THE REPORT	11
V. PROCESSING OF BREACH REPORTS. INVESTIGATORY PROCEEDINGS	13
VI. PROTECTION OF CONFIDENTIALITY; PROHIBITION OF RETALIATORY ACTIONS	16
VII. EXTERNAL REPORTS	19
VIII. REGISTER OF BREACH REPORTS	21
IX. PERSONAL DATA PROCESSING	22
X. FINAL PROVISIONS	24

With the aim of:

- contributing to the prevention of unlawful acts or omissions, or acts aimed at breaching the law, or the prevention of other breaches—including those concerning internal regulations in force within the Company as well as procedures and ethical standards adopted by the Company and the Capital Group—and thereby identifying irregularities related to such breaches in the activities of the Company and/or Subsidiaries;
- contributing to the prevention of potential threats and damages, and detecting potential or actual dangers and threats to the broad public interest as well as the interest of the Company, which would otherwise remain undetected;
- Striving to foster a culture of internal whistleblowing across the Capital Group in which employees report irregularities and violations of laws, procedures, internal regulations, and ethical standards as an expression of concern for the public interest and the well-being of the Company and its Subsidiaries, while also encouraging identified (non-anonymous) reporting, provided that robust and effective confidentiality safeguards are ensured.”
- Extending protection to Reporting Persons against retaliation where, at the time of submitting the report, they had reasonable grounds to believe that the reported information was true and that it related to a breach of law.
- Developing the Company’s management system in line with corporate social responsibility (CSR) principles, through conscious and sustainable actions that focus not only on financial performance and economic considerations, but also on addressing the needs and expectations of a broad range of social interests, including those of Employees and other stakeholders.

This Procedure is hereby adopted and implemented.

I. GENERAL PROVISIONS

§ 1

The Procedure defines:

1. Pursuant to § 1 and in implementation of the Act and Directive (EU) 2019/1937, this Procedure sets out the rules and process for reporting Breaches by Whistleblowers through dedicated and independent communication channels, handling reports, and taking appropriate follow-up actions in a manner that ensures the protection of the personal data of Whistleblowers, persons assisting in making a report, and persons connected with the Reporting Person, and protects such persons against retaliation, discrimination, coercion, or any other form of unfair treatment resulting from the reporting of a Breach.
2. Pursuant to Article 97d of the Public Offering Act, this Procedure also establishes the rules for anonymous reporting by Whistleblowers to a designated member of the Management Board and, in exceptional cases, to the Supervisory Board, concerning Breaches, in particular breaches of the Public Offering Act, Regulation (EU) 2017/1129, and the procedures and ethical standards applicable within the Company and the Capital Group.

The Procedure is simultaneously aimed at ensuring that Whistleblowers who report Breaches (as well as persons assisting in making the Report or persons connected with the Reporting Person) are protected against repressive actions, discrimination, or other types of unfair treatment.

§ 2

1. Whenever a given term is capitalized in the Procedure, it has the meaning assigned below:
 1. **Company Normative Act** – means any internal regulations in force within the Company or Subsidiaries, including policies, bylaws, procedures, internal orders, resolutions, ethical standards, and operational practices that regulate matters related to the business conducted by the Company;
 2. **Directive 2019/1937** – means Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law (Official Journal

of the EU L 305, 26.11.2019, p. 17, and Official Journal of the EU L 347, 20.10.2020, p. 1);

3. **Retaliatory Action** – means any direct or indirect action or omission caused by the Report that violates or may violate the rights of the Reporting Person (as well as persons assisting in making the Report or persons connected with the Reporting Person) or causes or may cause damage to the Reporting Person (as well as persons assisting in making the Report or persons connected with the Reporting Person); the details of prohibited retaliatory actions (or omissions) are set forth in § 18 et seq. of this Procedure;
4. **Capital Group** – means the Rainbow Tours Capital Group, comprising the parent company, i.e., Rainbow Tours Spółka Akcyjna, and all consolidated Subsidiaries;
5. **Client** – means any natural person, legal entity, or organizational unit without legal personality that has entered into, or intends to enter into, an agreement or transaction with the Company or a Subsidiary in connection with any legal relationship
6. **Labour Code** – means the Act of June 26, 1974, Labour Code (consolidated text: Journal of Laws of 2023, item 1465, as amended);
7. **Polish Code of Commercial Companies and Partnerships** – means the Act of September 15, 2000, Polish Code of Commercial Companies and Partnerships (consolidated text: Journal of Laws of 2024, item 18, as amended);
8. **Commission** – means an organizationally independent entity (internal body) of the Company appointed by the Company's Management Board or Supervisory Board (in matters concerning Reports

regarding Management Board members), authorized to take follow-up actions related to the Report, including: preliminary analysis and verification of the Report, conducting investigatory proceedings, further communication with the Reporting Person—including requesting additional information and providing feedback to the Reporting Person regarding the Report;

9. **Investor Relations Consultant** – means a person employed by the Company in the position of Investor Relations Consultant;
10. **Contractor** – means a natural person, legal person, or organizational unit without legal personality to which the law grants legal capacity, cooperating with the Company or a Subsidiary or interested in cooperating with the Company or a Subsidiary;
11. **Misuse or Breach** – means any act, omission, negligence, or other factual circumstance that violates, may lead to a violation of, or otherwise constitutes a breach of generally applicable laws, internal regulations, or ethical standards applicable within the Company, in a work-related context, i.e., in connection with an employment relationship or any other legal relationship forming the basis for the performance of work under which information about the Breach was obtained, including in particular: a) breaches relating to the areas specified in § 4(2) of this Procedure; b) breaches of the Public Offering Act and Regulation (EU) 2017/1129; c) breaches of ethical standards and internal normative acts applicable within the Company, as well as any act, omission, or negligence that constitutes, or may constitute, unlawful, illegal, or unethical conduct, including conduct related to the preparation, attempted commission, or

commission of a criminal offence within the meaning of the Act of 6 June 1997 – the Penal Code (consolidated text: Journal of Laws of 2020, item 1444, as amended), and conduct posing a particular risk to Employees, Contractors, or the Company. An illustrative list of acts or omissions that may constitute Misuse within the meaning of this Procedure is set out in § 4 of the Procedure.

12. **Recipient** – means the person or body within the Company authorized to receive Breach Reports, as referred to in § 6(3) of this Procedure, namely the designated member of the Management Board (subject to § 6(4) of this Procedure) and, in exceptional cases, including reports concerning members of the Management Board, the Supervisory Board.” exceptional cases, including reports concerning members of the Management Board, the Supervisory Board.” the designated member of the Management Board (subject to § 6(4) of this Procedure) and, in exceptional cases, including reports involving members of the Management Board, the Supervisory Board.” ;
13. **Central Authority** – means the authority referred to in Article 2(6) and Article 36(1) of the Act, namely the public authority responsible for providing information and support in relation to the reporting and public disclosure of breaches of law, as well as for receiving external reports concerning breaches of law in the areas covered by the Act, carrying out their preliminary assessment, and forwarding them to the competent authorities for further follow-up action. The Central Authority is the Commissioner for Human Rights
14. **Public Authority** – means the authority referred to in Article 2(7) and Article 36(2) and (3) of the Act, namely

a public administration authority that has established a procedure for receiving external reports concerning breaches of law within the scope of its statutory competence.

15. **Subsidiary Entity** – means a subsidiary of the Company within the meaning of the Accounting Act of 29 September 1994 (consolidated text: Journal of Laws of 2021, item 217), i.e., a commercial company or an entity established and operating under foreign commercial law that is controlled by the Company as the parent entity.
16. **Employee** – means any person employed by the Company under an employment contract and qualifying as an employee within the meaning of Article 2 of the Labour Code, as well as any temporary worker assigned to work for the Company within the meaning of Article 2(2) of the Act of 9 July 2003 on the Employment of Temporary Workers (consolidated text: Journal of Laws of 2019, item 1563
17. **Procedure** – means this Internal Procedure for Reporting Breaches of Law and Other Irregularities, Taking Follow-up Actions, and Defining the Conditions for the Protection of Persons Reporting Breaches at Rainbow Tours S.A., as applicable within the Company.
18. **Supervisory Board** – means the supervisory body of the joint-stock company operating under the name Rainbow Tours Spółka Akcyjna;
19. **Register of Breach Reports** – means the register of Breach reports referred to in § 14 of the Procedure;
20. **Regulation 2016/679 or GDPR** – means Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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) (Official Journal of the EU L 119);

21. **Regulation 2017/1129** – means Regulation (EU) 2017/1129 of the European Parliament and of the Council of June 14, 2017, on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC (Official Journal of the European Union L 168/12);

22. **Regulation 596/2014 or MAR** – means Regulation (EU) No 596/2014 of the European Parliament and of the Council of April 16, 2014, on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (Official Journal of the EU L 173/1);

23. **Company or Employer** – means Rainbow Tours Spółka Akcyjna with its registered office in Łódź (90-361) at ul. Piotrkowska 270, entered into the Register of Entrepreneurs of the National Court Register under KRS number 0000178650, NIP: 7251868136, REGON: 473190014, acting as an employer within the meaning of Article 3 of the Labour Code;

24. **Act** – means the Act of June 14, 2024, on the Protection of Whistleblowers (Journal of Laws of 2024, item 928) implementing Directive 2019/1937 into the Polish legal order;

25. **Public Offering Act** – means the Act of July 29, 2005, on Public Offerings and Conditions Governing the Introduction of Financial Instruments to Organised Trading Systems and on

Public Companies (consolidated text: Journal of Laws of 2024, item 620);

26. **Management Board** – means the managing body (Management Board) of the -public company operating under the name Rainbow Tours Spółka Akcyjna;

27. **Reporting Person or Whistleblower** – means a person making a Breach report, provided that internal reports made on the basis of this Procedure and under the mode covered by the Procedure are accepted from a natural person having the status of:

a) an Employee, and also:

b) a former employee of the Company, i.e., a person previously employed by the Company under an employment relationship, where the employment relationship has already ceased,

c) a person employed by the Company under a civil-law contract (e.g., a specific-task contract or mandate contract),

d) an entrepreneur conducting business personally and on a sole-proprietorship basis in a relationship with the Company (including under a "B2B" cooperation agreement),

e) a job applicant who learned of a Breach during the recruitment process or during negotiations prior to entering into an employment contract, civil-law contract, or cooperation agreement;

f) an intern, trainee, or volunteer at the Company;

g) a member of the Management Board or Supervisory Board;

h) a commercial proxy, shareholder, or partner;

28. **Report or Internal Report** – the transmission of information regarding an actual Breach, a potential Breach, or a reasonable suspicion of a Breach to the Employer by a Whistleblower, using the communication channels designated in this Procedure

29. **External Report** – the transmission of information regarding a Breach by a Whistleblower to a Public Authority or

Central Authority, in the manner and through the communication channels established by those authorities.

2. Definitions and terms used in the Procedure in the singular also apply to the plural, unless the Procedure explicitly states otherwise or it results from the context.

II. SCOPE OF THE PROCEDURE

§ 3

1. The purpose of the Procedure is:
 1. to establish and apply uniform rules for reporting actual or threatened illegal, unethical, or unlawful acts, as well as actions posing a particular risk to the social and public interest, the interests of Employees, Clients, Contractors, the Company, or any Subsidiary, and to define the framework for taking follow-up actions;
 2. to ensure effective action is taken to halt such practices, as well as potential breaches of the law, internal Company Normative Acts, procedures, and ethical standards adopted within the Company and the Rainbow Tours Capital Group.
2. This Procedure applies without prejudice to the obligation of Employees, Management Board members, and Supervisory Board members to comply with all mandatory laws and legal provisions currently in force.
3. The making a Report in good faith shall not result in any Retaliatory Actions or other adverse measures against the Whistleblower. The Whistleblower—along with any person assisting with the Report or connected to the Reporting Person within the meaning of the relevant provisions of the Act—is protected under this Procedure and Chapter 2 of the Act, provided they had reasonable grounds to believe that the information regarding the reported Breach was true at the time of the Report and that such information constituted a Breach.

4. Whistleblowers who submit reports in bad faith, file frivolous reports, or make reports that constitute an abuse of rights are not protected under this Procedure (nor under the relevant provisions of the Act). Such protection is also denied to any Whistleblower who knowingly and intentionally provides false or misleading information when making a Report.

§ 4

1. This Procedure covers any actual or potential Breach, the risk of a Breach, or any attempt to conceal a Breach related to the Company's business operations that has occurred or is likely to occur within the Company or in connection with its activities. Specifically, it encompasses any factual situation—including acts or omissions—that violates, potentially leads to the violation of, or circumvents applicable laws, internal regulations, or ethical standards in force within the Company, within a work-related context (meaning circumstances connected with an employment relationship or any other legal relationship serving as the basis for performing work, through which information regarding a Breach was obtained).
2. Subject to the provisions of the following paragraph, the material scope of this Procedure covers any Breach that constitutes an unlawful act or omission, or one aimed at circumventing the law, particularly in the areas of:
 1. corruption;
 2. public procurement;
 3. financial services, products, and markets;
 4. prevention of money laundering and terrorist financing;
 5. product safety and compliance;
 6. transport safety;
 7. environmental protection;
 8. radiological protection and nuclear safety;

9. food and feed safety;
 10. animal health and welfare;
 11. public health;
 12. consumer protection;
 13. protection of privacy and personal data;
 14. security of network and information systems;
 15. financial interests of the European Union;
 16. internal market of the European Union, including competition and state aid rules as well as corporate taxation;
 17. constitutional freedoms and human and citizen rights.
3. Other Breaches falling within the material scope of this Procedure—including Breaches of internal regulations in force within the Company (Company Normative Acts) or ethical standards—also encompass Breaches related to and arising from the business conducted by the Company, specifically including:
1. crimes committed by Employees against Clients or Contractors, including embezzlement of funds belonging to a Client or Contractor;
 2. misdemeanors and offenses against Employee rights, including discrimination, mobbing, sexual harassment, harassment, discrimination based on gender, age, racial/ethnic origin, religious affiliation, sexual orientation, worldview, as well as exposing the health and life of Employees to danger through failure to guarantee the right to safe and hygienic working conditions or violation of safety rules;
 3. corruption, bribery (active and passive), i.e., demanding, accepting, promising, offering, giving, or soliciting material or non-material benefits in

- exchange for unethical, illegal action violating trust, e.g., selecting a bidder or service provider for the Company in exchange for accepting a financial or non-financial benefit (bribe);
4. defalcation, i.e., unethical and/or illegal conduct aimed at obtaining an unlawful or unfair advantage, causing damage or loss to the Company, a Subsidiary Entity, or third parties, e.g., unjustified purchases made for private needs using a credit card issued to the Company or a Subsidiary Entity, inflating employee expenses, etc.;
 5. actions detrimental to the Company, including the intentional causing of workplace accidents, unjustified sick leave, embezzlement, destruction or theft of Company property, use of Company assets for purposes unrelated to official duties, unjustified corporate purchases (including paying for objectively unnecessary or fictitious services), and abuse of office or position.
 6. falsification of documentation, accounting fraud, e.g., falsification of financial statements, falsification of invoices, falsification of accounting documents, forging signatures on documents;
 7. nepotism, cronyism, i.e., e.g., unjustified favoritism towards family members/acquaintances when filling positions, recruitment, paid patronage;
 8. theft, destruction of property, including e.g., theft or intentional destruction of property of the Company or a Subsidiary Entity;
 9. theft, disclosure, or use of legally protected information, including information constituting a business secret within the meaning of Article 11 of the Act of April 16, 1993, on Combating Unfair Competition

(consolidated text: Journal of Laws of 2020, item 1913, as amended), inside information within the meaning of Article 7 of Regulation 596/2014 (MAR), or personal data within the meaning of the provisions of Regulation 2016/679 (GDPR);

10. other improper or unethical behaviors that remain in contradiction with values resulting from ethical principles in force in the Company, including those resulting from the following Company Normative Acts in force in the Company: "Rainbow Tours Capital Group Social Policy", "Rainbow Tours Capital Group Environmental Policy", "Rainbow Tours Capital Group Personnel Policy", "Rainbow Tours Capital Group Human Rights Policy", "Rainbow Tours Capital Group Anti-Corruption Policy", "Rainbow Tours Capital Group Diversity Policy".

4. The Company encourages Whistleblowers to direct information about a Breach to the Company in the first instance, especially with regard to the types of Breaches referred to in paragraph 3 of this paragraph of the Procedure.

§ 5

1. This Procedure does not apply in the following situations:

1. if information on a Breach has been reported on the basis of separate legal provisions, in particular as a complaint or notification of a suspected crime—while the Employer urges potential Whistleblowers to use internal reporting in the first instance under the provisions of this Procedure, utilizing internal channels for reporting Breaches;

2. With regard to the perpetrator of a breach of law, this Procedure applies without prejudice to any statutory exemptions from liability or penalty reductions they may be entitled to based on their post-breach conduct—in particular, through the voluntary disclosure of the breach

or cooperation with law enforcement agencies or other competent authorities.

2. This Procedure shall not apply if the reported Breach prejudices exclusively the rights of the Reporting Person or is submitted solely in the individual interest of the Whistleblower (for example, a dispute regarding an individually miscalculated salary rather than a systemic issue), which should instead be handled through standard, customary employment or administrative procedures.

III. REPORTING BREACHES; RULES FOR NOTIFYING BREACHES

§ 6

1. Anyone entitled under the Procedure to submit a Breach report (Whistleblower), provided they have a reasonable suspicion of the occurrence or potential occurrence of a Breach and reasonable grounds to believe that the information or knowledge possessed is true at the time of submitting the Report, and that such information constitutes information on a Breach, acting in good faith, may notify of Breaches occurring or potentially occurring in the Company or in Capital Group companies (Subsidiary Entities).

2. **The internal entity authorized to receive Internal Reports (Recipient)** is, as a rule, the Company's **Management Board**. In the case of Reports concerning members of the Management Board, this entity is the Company's **Supervisory Board**.

3. Reports shall be transmitted to the Recipient (i.e., for the attention of the designated Management Board member, and in special cases—including Breaches concerning Management Board members—to the Supervisory Board) in the manner indicated in § 7 of this Procedure.

4. The designated member of the Management Board is the President of the Management Board, unless the Management Board indicates another Management Board member by way of a resolution.

5. The Recipient (the designated member of the Management Board or Supervisory Board) is required to handle the matter with due diligence, impartiality, meticulousness, and objectivity, while strictly maintaining confidentiality and adhering to the deadlines set forth in this Procedure. This includes ensuring that a preliminary analysis and verification of the reported information are performed, and overseeing the subsequent processing of the Report and the implementation of appropriate follow-up actions with the participation of a dedicated Commission appointed pursuant to Chapter IV of this Procedure. Furthermore, the Recipient must confirm receipt of the Report to the Whistleblower within 7 days of its receipt, unless the Whistleblower has failed to provide a contact address for this purpose.
6. In the event that the Breach Report concerns a member of the Management Board and has not been reported directly to the Supervisory Board, the matter is forwarded to the Supervisory Board for the purpose of its further processing.
7. Members of the Management Board and the Supervisory Board acting as Recipients are authorized to receive and verify Reports, take follow-up actions, and process the personal data of both the Whistleblower and the data subjects exclusively on the basis of written authorization from the Company, as referred to in § 17, paragraph 2 of this Procedure.

§ 7

1. A Reporting Person who intends to notify the Recipient of a Breach may use the following communication means (channels):
 1. **traditional postal form** sent to the Company's correspondence address: **Rainbow Tours S.A., ul. Piotrkowska 270, 90-361 Łódź**, in a shipment in two envelopes: a closed envelope (internal) marked with the inscription **"Confidential. Whistleblower Report"** placed in another closed envelope (external) addressed to the appropriate

Recipient (in accordance with § 6 paragraph 3 and paragraph 4 of the Procedure);

2. **an internal communication system utilizing physical drop boxes** (known as "Trust Boxes"), through which the Reporting Person submits a Breach report in a sealed envelope marked *"Confidential – Whistleblower Report"*, addressed either to:

a) the "Management Board Trust Box," if the Reporting Person wishes to report a Breach to the designated Management Board member, or

b) the "Supervisory Board Trust Box," if the Reporting Person wishes to report a Breach to the Supervisory Board. ;

3. via **dedicated e-mail addresses**, to the e-mail address: a) **zgloszenie.zarzad@r.pl**, when the Whistleblower reports a Breach to the designated Management Board member, or b) **zgloszenie.radanadzorcza@r.pl**, when the Whistleblower reports a Breach to the Supervisory Board; however, solely and exclusively in the event that the Reporting Person consents to and wishes to disclose their identity, as such a method of notification does not guarantee the preservation of the Whistleblower's anonymity.

2. The use of communication channels other than those specified in the preceding paragraph for matters related to Breach Reports—such as dedicated IT software, an email inbox, or an electronic submission form that enables the anonymization of the Reporting Person's data, with access restricted exclusively to the designated Management Board member and/or the Supervisory Board—requires a separate decision by the Management Board and prior notification to Employees regarding the implementation of such a channel.

1. The basic rules regarding the reporting of Breaches are as follows:

1. **Breach reports may be made anonymously**, but as a rule, the Whistleblower should state their identity and additionally their address (preferred feedback contact method) in order to enable communication with the Whistleblower whenever necessary for the proper and adequate handling of a Report, conducting potential investigatory proceedings, or taking other follow-up actions related thereto; t;

2. it is recommended, for the purpose of examining the Report in a reliable manner and enabling the adoption of adequate actions, to include and provide the following information in the Report:

- **the name of the Company's organizational unit or the name of the Subsidiary Entity** to which the Report relates,
- **the type of Breach or the area to which the Breach relates**, indicated in particular taking into account the scope and types of Breaches or Breach areas listed in § 4 of the Procedure,
- **a description and date (or approximate period) of the event constituting the Breach or potential Breach and the circumstances of its occurrence**, i.e.: a description of the matter/event to which the Report relates, indicating all known, relevant facts significant to the matter (what happened or may happen, where, when, and what exact behaviors were the reason for the Report), an indication of the interest that, in

the Reporting Person's opinion, is or may be violated (e.g., the interest of Employees, the interest of the Company, the interest of a Subsidiary, the interest of a Client, the interest of a Contractor),

- **a description of the method of acquiring information** about the matter/event,
- **persons involved in the reported Breach**, i.e.: indicating who is involved in the matter or responsible for it, providing the name and surname of each such person; indicating whether the matter was reported to a superior along with a description of the superior's reaction to the report (indicating actions taken by the superior, i.e., whether the superior tried to clarify the matter, or ignored or covered it up),
- any other existing elements important for the reported matter that may be helpful in clarifying the matter, and in particular, if possible, **documents or other information** that may confirm the occurrence of the Breach,
- details of the Reporting Person: name and surname, contact details (indicating the preferred feedback contact method while ensuring the safeguarding of the principle of anonymity, e.g., by using dedicated and private e-mail address of the Whistleblower, which was created specially for this purpose)
 - **NOTE! providing this data is entirely voluntary and remains at the sole discretion of the Reporting Person;**

3. the Report should be transmitted by the Reporting Person as soon as possible from the moment of occurrence or identification of the Breach;
 4. failure by the Whistleblower to provide all information in the Report referred to in item 2) above does not release the Recipient from the obligation to examine the Report.
2. **Authorized persons, i.e., persons responsible for receiving Reports, have an absolute obligation to maintain confidentiality of all data concerning the Reporting Person or other information that could lead to the disclosure or cause the disclosure of the Reporting Person's identity.** The personal data of the Reporting Person and other data allowing for the establishment of the Reporting Person's identity may be disclosed only with the explicit consent of the Reporting Person.
3. The Reporting Person should refrain from using or abusing the Procedure for the purpose of intentionally harming other Employees, Clients, Contractors, the Company, or Subsidiary Entities; the Reporting Person should act in good faith; the Reporting Person is in good faith if they have a justified conviction of the existence of a Breach and demonstrate that they had reasonable grounds to believe that the information on the Breach constituting the subject of the Internal Report was true at the time of making the Report and that such information constituted information on a Breach.
4. The Company will not tolerate the deliberate or intentional misuse or abuse of this Procedure for actions undertaken in bad faith and with malicious intent, in violation of the duty referred to in the preceding paragraph—such as filing retaliatory complaints to undermine, slander, or

§ 11

1. The Company is required to take all follow-up actions related to the Report with due diligence, impartiality, meticulousness, and objectivity,

discredit co-workers. Only reliable information relevant to the functioning of the organization and submitted in good faith (*bona fide*) should be reported.

§ 9

1. The "trust boxes" referred to in § 7 paragraph 1 point 2) of the Procedure are placed at the Company's registered office, i.e., in Łódź, at the address: 90-361 Łódź, ul. Piotrkowska 270, in a publicly accessible place (or publicly accessible places), unequipped with a monitoring and access control system.
2. The contents of the "trust boxes" are checked on an ongoing basis, no less frequently than once a week, by the Recipient or by a person authorized by the Recipient, and in the latter case, in an intact form, they are subject to immediate transmission to the appropriate Recipient or Recipients.
3. The act of transmitting the report to the Recipient is recorded in the Register of Breach Reports.

§ 10

1. The Company is obliged **to confirm to the Reporting Person the receipt of the Report within 7 (seven) days from the date of its receipt**, unless the Reporting Person has not provided an address or communication channel to which or via which the confirmation should be transmitted.
2. The confirmation referred to in the preceding paragraph is transmitted to the Reporting Person **by the Recipient or by the Commission**, to the address or via the communication channel indicated by the Whistleblower in the Report.

IV. PRELIMINARY ANALYSIS AND VERIFICATION OF THE REPORT

while strictly maintaining confidentiality and adhering to the deadlines set forth in this Procedure.

2. The Company shall take all legally permissible actions to obtain, prior to any potential classification of the Report as "not subject to examination" or "unexamined", the information and documents necessary for its effective examination.
3. All reported Breaches, regardless of whether they were committed by management staff, managing or supervising persons, or other Employees, shall be treated with equal seriousness and objectivity.

§ 12

1. **The organizationally independent internal body authorized to take follow-up actions related to a Report**—including preliminary analysis and verification, deciding whether to further process the Report or dismiss it without examination, conducting investigatory proceedings, and communicating further with the Reporting Person (such as requesting additional information and providing feedback)—is **a dedicated Commission** appointed by:
 - the Supervisory Board—in the case of Reports concerning members of the Management Board, or
 - the Management Board—in the case of all other Reports.

Persons appointed to the Commission are authorized to receive and review Reports, take follow-up actions, and carry out any related processing of personal data concerning Whistleblowers and persons identified in the Reports, solely on the basis of a written authorization issued by the Company referred to in § 17(2) of the Procedure. **Authorized persons (i.e., those responsible for conducting investigations) are strictly obliged to maintain the confidentiality of all information concerning the Reporting Person and any other information that could reveal, directly or indirectly, the Reporting Person's identity.** The personal data of the Reporting Person, as well as any other information enabling the identification of the Reporting Person, may be disclosed only with the Reporting Person's explicit consent.

2. The Commission shall consist of at least two persons selected from among the Company's

Employees and/or members of the Management Board or Supervisory Board. The members of the Commission shall be appointed on a case-by-case basis (i.e., for the examination of a specific Report) by the Management Board; however, in the case of a Report concerning a member of the Management Board, the Commission shall be appointed by the Supervisory Board. The Commission shall be composed in a manner that ensures an objective, independent, and thorough examination of the matter covered by the Report. The Investor Relations Consultant shall be a permanent member of the Commission, including by virtue of serving as the person responsible for maintaining the Register of Breach Reports.

3. As a rule, the Chairperson of the Commission shall be a person appointed by, and selected from among the members of, the body that appoints the Commission (in accordance with paragraph 1). However, after the Commission has been appointed, and provided that all members unanimously agree, the Commission may elect another person to serve as its Chairperson.
4. To ensure the transparency and independence of the proceedings, at least one person who is not a member of the Management Board or the Supervisory Board should, as a rule, be appointed to the Commission. However, in straightforward, minor, or less complex matters, or in matters requiring a lower level of involvement, the Commission may be composed exclusively of members of the Company's Management Board and/or Supervisory Board (and, where the Report concerns a member of the Management Board, without the participation of the other Management Board members), acting as the persons responsible for receiving the Report. The decision to apply this simplified verification procedure shall be made by the designated member of the Management Board or, as the case may be, by the Supervisory Board.
5. A person may not serve as a member of the Commission if the Report concerns that person, if the person is the direct supervisor of the

Whistleblower or of the person concerned by the Report, or if the person is directly subordinate to the Whistleblower or to the person concerned by the Report. If, in the opinion of a Commission member, any circumstances arise that could affect that member's impartiality in assessing the Report, or give rise to a conflict of interest, even a potential one, the member is required to withdraw from the Commission's work in the investigatory proceedings. In such a case, where necessary, the authorized body shall appoint a new member to replace the member who has withdrawn or has been excluded from the Commission's work.

6. At the stage of the preliminary analysis and verification of a Report and/or during further investigatory proceedings, the Commission may consider involving representatives of various organizational units of the Company or an independent consultant, if, in the Commission's opinion, their knowledge and experience are necessary for the preliminary assessment and verification of the Report and/or for conducting and implementing the further investigatory proceedings. Members of the Commission shall be granted authorization, on a case-by-case basis, to process the personal data covered by the Report.

§ 13

1. Upon receipt of the Report and appointment of the Commission, the Report is examined in accordance with the principles set out in the Procedure.
2. The Commission shall first conduct a preliminary review and verification of the Report, in particular to assess whether the information contained in the Report is sufficient to examine its merits. Where necessary, and if possible, the Commission shall contact the Whistleblower.
3. After conducting the preliminary analysis and verification of the content of the Report (taking

V. PROCESSING OF BREACH REPORTS. INVESTIGATORY PROCEEDINGS

§ 14

into account, among others, the material scope defined in § 4 of the Procedure), the Commission may decide to refrain from conducting and continuing the investigatory proceedings in the event that:

1. the nature or subject matter of the Report justifies leaving it without further examination due to the absence of grounds for applying the Procedure or the existence of obstacles preventing the application of the Procedure, in accordance with § 5 of the Procedure; or
 2. the Report is obviously unfounded or unreliable, or
 3. the Report was made in bad faith, or
 4. it is impossible to obtain even partial information relating to the Report that is necessary to conduct the investigatory proceedings and that would allow, at least to some extent, the examination and verification of the Report; or
 5. the Breach covered by the content of the Report is not subject to the protection provided for in the Procedure (also provided for on the basis of the relevant provisions of the Act).
4. Refraining from conducting and continuing investigatory proceedings requires an appropriate annotation in the Register of Breach Reports.
 5. If the content of the Report enables the analysis and verification of the merits of the Report, and furthermore, according to the information covered by the Report, there is a probability of the occurrence of a Breach or other irregularities, the Commission decides to initiate and implement investigatory proceedings.
 1. The Commission examines the Report, takes follow-up actions, and provides feedback without undue delay. **The maximum deadline for providing feedback to the Reporting Person shall not exceed 3 (three) months**

counting from the confirmation of receipt of the Report or—in the event of failure to transmit confirmation to the Reporting Person—counting from the expiry of **7 (seven)** days from the date of making the Report. The feedback includes, in particular, information on the determination or non-determination of the occurrence of a Breach and any measures that have been or will be applied in response to the ascertained Breach.

2. The Commission fulfills the information obligation resulting respectively from Article 13 or Article 14 of the GDPR toward persons whose personal data are processed in the process of verifying Reports. The above obligation does not apply to Whistleblowers who have made a Report anonymously.
3. The Commission verifies the merits of the Report in investigatory proceedings based on internal acts in force in the Company (including the Company's Normative Acts) and information obtained in the course of proceedings from representatives of the Company's organizational units, taking into account the type and nature of the Report and subject to the preservation of confidentiality. Investigatory proceedings are conducted with due diligence, impartially, meticulously, objectively, and within the deadlines indicated in this Procedure.
4. Where necessary, the Commission may invite Whistleblowers (to the extent that they have provided their contact details and the Report is not anonymous), as well as Employees and other co-workers of the Company (including persons engaged under civil law contracts, sole proprietors providing services to the Company, including under B2B cooperation agreements, and other similar persons) who may be connected with the matter or possess any actual or potential knowledge relating to the matter or information described in the Report. At the Commission's request, each such person is required to attend the Commission's meeting and provide any necessary documents and

information needed to establish all the circumstances related to the Report.

5. For the purpose of ensuring a reliable and proper verification or examination of a Breach Report, the Commission may, in justified cases and taking into account the need to limit the scope of the information disclosed in light of the objectives of the Procedure and the content of the Breach Report, decide to seek professional or expert assistance from third parties where specialist knowledge is required. In such a case, the third party (expert) may participate in the examination of the matter and shall be obliged to maintain the confidentiality of the course and results of the investigatory proceedings, as well as of all documents and statements obtained in the course of those proceedings. The relevant provisions of the Procedure shall apply accordingly to such third parties.
6. During the preliminary analysis and verification of the Report, the Commission determines whether the reported matter is subject to examination and takes the actions indicated in § 13 of the Procedure.
7. After establishing all relevant facts and reaching a decision on the merits of the Report, the Commission shall make recommendations regarding appropriate corrective or disciplinary measures to be taken against the person or persons concerned who committed the Breach. Where appropriate, the Commission may also recommend preventive measures aimed at preventing similar Breaches from occurring in the future. The Commission shall submit its recommendations to the Management Board or the Supervisory Board, as applicable.
8. In the event of recognizing the reported Breach as well-founded and subject to examination within the framework of the Procedure, after conducting and as a result of conducting the investigatory proceedings, necessary actions are undertaken, including, for example, adequate (i.e., if required or justified) actions aimed at:

- convening a session of the Management Board or a session of the Supervisory Board,
 - issuing necessary instructions to Employees aimed at preventing the occurrence or further occurrence of Breaches,
 - undertaking potential remedial or disciplinary measures toward persons committing the Breach,
 - submitting a notification of the possibility of committing a crime to competent authorities in the manner provided for by relevant legal provisions, if in the course of investigatory proceedings the Commission deems it authorized and well-founded.
9. If the reported Breach is deemed well-founded and eligible for review under the Procedure, following the completion of the investigation, the Chairman of the Commission shall, where appropriate:
- forward the outcome of the investigation to the head of the Company's organizational unit in which the person indicated in the Report or the Whistleblower performs their duties, or to the Management Board member directly supervising the person indicated in the Report or the Whistleblower, in order to take appropriate follow-up corrective or disciplinary actions against the person to whom the Breach Report relates, as indicated in the Commission's protocol and provided for by the work regulations applicable to the person indicated in the Report, resulting from an individual cooperation agreement, or arising from generally applicable laws; and
 - inform the employee, collaborator, or other person to whom the Report relates and who is accused of committing a Breach about the submitted Report, the verification

of the Report carried out (the investigation), and the disciplinary and/or corrective and remedial measures taken.

10. In the event that as a result of investigatory proceedings it is stated that the reported Breach did not occur, or it failed to gather sufficiently certain evidence testifying to the occurrence of the Breach, the Commission decides to discontinue the investigatory proceedings, which simultaneously is subject to an appropriate entry in the Register of Breach Reports.
11. If the Report is found to be unsubstantiated, or if the investigatory proceedings establish that the reported Breach did not occur or that there is insufficient reliable evidence to confirm that the Breach occurred, the Chairperson of the Commission shall promptly inform the Whistleblower and the Employee, co-worker, or member of the Company's Management Board to whom the Report relates of the Report and the verification carried out in connection with it (i.e., the investigatory proceedings). If the Report concerns a member of the Company's Management Board, the Chairperson shall also inform the Supervisory Board of the completion and outcome of the investigatory proceedings.
12. Follow-up actions taken after the completion of investigatory proceedings concerning a Breach should be appropriate and proportionate. When assessing the appropriateness of such actions, particular consideration should be given to the measures taken to verify the information concerning the Breach, the accuracy of the assessment of that information, and the adequacy of the measures taken following the establishment of the Breach, including, where appropriate, measures aimed at preventing further Breaches, taking into account the seriousness of the Breach. Closing the procedure for verifying information concerning a Breach on the grounds that the Breach was clearly minor and did not warrant any further follow-up action shall also be considered an appropriate follow-up action.

§ 15

1. Sessions of the Commission are recorded in each time in the report. Explanations provided by summoned persons are recorded, in particular by making appropriate entries in the session report of the Commission or in a separate document. Protocols from sessions or documentation collected during Commission sessions are maintained and archived—while maintaining confidentiality principles—by the Investor Relations Consultant, including in the Register of Breach Reports.
2. If the Commission is unable to reach a unanimous decision, its final conclusions and other decisions shall be adopted by a simple majority of votes. In the event of a tie, the Chairperson of the Commission shall have the casting vote and shall, as a rule, cast their vote last.
3. Final conclusions agreed upon by the Commission contain in particular a description of the facts, a decision regarding the merits of the Report, and—if the Reports is recognized as well-founded—recommendations concerning appropriate follow-up and/or preventive actions.
4. When the Report concerns a member of the Company's Management Board, the chairperson of the Commission transmits the final report to the Supervisory Board, which has the ability and is authorized to address the findings, of which it immediately informs the chairperson of the Commission.

§ 16

Members of the Commission, as well as all other authorized persons participating in the process of preliminary analysis and verification of the Report and in investigatory proceedings regarding the verification and examination of the Breach Report, in accordance with the principles indicated in §§ 11–15 of the Procedure, until the completion of conducted proceedings (and also in subsequent periods, if necessary due to the nature of the matter covered by the Report) are obliged to act in a manner ensuring the avoidance of suspicion among persons against whom investigatory and verification

proceedings have been initiated, avoiding at the same time statements that could negatively impact the image of the Company or persons or entities associated with it.

§ 17

1. The person to whom the Report relates is entitled to obtain information on the subject matter of the case and to submit explanations, insofar as it is objectively possible in a given case.
2. The right to obtain information referred to in paragraph 1 above does not entitle the person to whom the Report relates to make copies of documents and other materials concerning the conducted investigatory proceedings, findings made, and measures undertaken, unless this is required by universally binding legal provisions, e.g., evidence in court proceedings, or by the Company's binding internal Normative Acts.

VI. PROTECTION OF CONFIDENTIALITY; PROHIBITION OF RETALIATORY ACTIONS

§ 18

1. The Company shall ensure the protection of the personal data of both the Whistleblower and any natural person to whom the Report relates, including the confidentiality of their identity throughout all stages of the proceedings concerning the Report. This shall be without prejudice to any obligation to disclose information arising under generally applicable laws in connection with investigative activities or subsequent disciplinary or judicial proceedings. **The obligation to maintain confidentiality also applies to any information that could directly or indirectly reveal the identity of such persons.**
2. The Company's Management Board is obliged to undertake **all actions aimed at preventing unauthorized persons from obtaining access to information covered by the Report and ensuring the protection of the confidentiality of the identity of the person making the Report and the person to whom the Report relates.** In particular, the Company ensures this by admitting to the reception and verification of Reports, undertaking follow-up

actions, and processing personal data of the Whistleblower and each natural person to whom the Report relates **exclusively persons with written authorization from the Company**, including in particular members of the Commission. **Authorized persons are obliged to maintain secrecy.**

3. The personal data of the Reporting Person shall be stored separately from the document or other medium containing the Report. Where appropriate, all personal data identifying the Reporting Person shall be removed from the Report or other medium immediately upon receipt. **Authorized persons (i.e., persons responsible for receiving Reports and conducting investigatory proceedings) shall be strictly obliged to maintain the confidentiality of all information concerning the Reporting Person and any other information that could directly or indirectly reveal their identity.** To protect the identity of the Reporting Person throughout the proceedings concerning the examination of the Report and the implementation of any follow-up actions, and to facilitate the conduct of such proceedings, the Reporting Person may be assigned a unique code name accessible only to authorized persons. The code name shall be used to identify the relevant Reporting Person for the purposes of the proceedings without disclosing their identity.
4. Personal data of the Reporting Person are stored in the Register of Breach Reports, in encrypted catalogs, separate from other information covered by the Report and archived in appropriate positions of the Register of Breach Reports.
5. Subject to the provisions of the preceding paragraph, all materials related to proceedings aimed at preliminary analysis and verification of the Report and its further examination and implementation of other follow-up actions related to the Report are stored in the Register of Breach Reports, in separate encrypted catalogs.

§ 19

1. The submission by a Reporting Person, in accordance with the Procedure, of information concerning a Breach shall not constitute grounds for imposing any adverse, retaliatory, or discriminatory measures against the Reporting Person. Any retaliation, discrimination, or other form of unfair treatment of a Whistleblower who, in good faith, submits a Report shall be considered a serious breach of the Procedure and may result in disciplinary measures or termination of the agreement between the Employee or co-worker and the Company, or termination of the cooperation, as applicable. Such conduct may also give rise to civil or criminal liability under applicable law, including the relevant provisions of the Act (Chapter 6, "Penal Provisions").
2. The Company does not tolerate repressive actions, discrimination, or other kinds of unfair treatment also toward persons assisting in making the Report and persons associated with the Reporting Person, within the meaning of relevant provisions of the Act, as well as toward other persons cooperating during internal investigatory proceedings related to the verification of the merits of the Breach Report.

§ 20

1. Any unfavorable treatment constituting unauthorized retaliation against a Whistleblower, a person assisting in the submission of a Report, or a person associated with the Whistleblower (provided that such person is also employed by the Company) shall, where work is or is to be performed under an employment relationship, in particular include:
 1. refusal to establish an employment relationship,
 2. notice of termination or termination of an employment relationship without notice,
 3. failure to enter into a fixed-term employment contract following the expiry of a probationary employment

contract, failure to enter into a subsequent fixed-term employment contract, or failure to enter into an indefinite-term employment contract following the expiry of a fixed-term employment contract, where the Employee had reasonable grounds to expect that such a contract would be entered into;

4. reduction of work remuneration,
5. withholding of promotion or omission in promotion,
6. omission in granting work-related benefits other than remuneration,
7. transfer of the employee to a lower position,
8. suspension from performing employment or official duties,
9. transfer of existing employee duties to another employee,
10. an unfavorable change in the place of work or the employee's working hours or work schedule,
11. negative evaluation of work results or negative opinion on work,
12. imposition or application of a disciplinary measure, including a financial penalty, or similar measure,
13. withholding or unjustifiably preventing participation in vocational training or other training aimed at improving professional qualifications,
14. unjustified referral for a medical examination, including a psychiatric examination, where applicable law provides for the possibility of referring an Employee for such an examination,
15. taking any action intended to prevent or hinder the Employee from obtaining employment in a particular sector or industry in the future on the basis of a formal or informal sectoral or industry

agreement, unless the Company, as the employer, demonstrates that such action was based on objective reasons.

2. Any threat or attempt to take any of the measures referred to in paragraph 1 shall also be considered unfavorable treatment on the grounds of having made a Report, unless the Company, as the employer, demonstrates that such action was based on objective reasons.

§ 21

Any unfavorable treatment constituting unauthorized retaliation against a Whistleblower, a person assisting in the submission of a Report, or a person associated with the Whistleblower (provided that such person is employed by the Company or otherwise performs work for the Company) shall, where work is or is to be performed under a legal relationship other than an employment relationship, in particular include the termination or attempted termination of, or refusal to enter into, the legal relationship under which the reporting person performs or is to perform work, unless the other party to that legal relationship demonstrates that such action was based on objective reasons. In such a case, any unilateral legal act terminating the legal relationship on the grounds that a Report was made shall be ineffective.

§ 22

1. Making a Report shall not constitute grounds for imposing disciplinary liability on the Reporting Person, provided that the Reporting Person had reasonable grounds to believe that making the Report was necessary to disclose a Breach in accordance with the Procedure or the Act.
2. Making a Report shall not constitute grounds for holding the Reporting Person liable, including for any damage, for violating the rights of others or obligations arising under applicable law, in particular in relation to defamation, infringement of personal rights, infringement of copyright, violation of personal data protection laws, or breach of a duty of confidentiality, including trade secrets, provided that the Reporting Person had reasonable grounds to believe that making the Report was necessary to disclose a

Breach in accordance with the Procedure or the Act.

3. Notice of termination or termination without notice of a contract in economic turnover to which the Reporting Person is a party, in particular concerning the provision of services, due to making a Report is ineffective.
4. Making a Report cannot constitute a basis for imposing an obligation or refusing to grant, restricting, or withdrawing an entitlement.
5. It is not possible to waive the rights specified in § 20 or § 21 or to assume liability for damage arising due to making a Report.
6. Any provision of an employment contract or other instrument establishing an employment relationship, or governing the rights and obligations of the parties to such relationship, shall be null and void to the extent that it directly or indirectly excludes or restricts the right to make a Report. The same shall apply to provisions of any other contract or instrument under which work is performed, to the extent that they directly or indirectly exclude or restrict the right to make a Report.

§ 23

1. Responsibility for protecting the Whistleblower, as well as any person assisting in the submission of a Report or any person associated with the Whistleblower (provided that such person is employed by the Company or otherwise performs work for the Company), shall rest with the Company's Management Board or, where the Report concerns a member of the Management Board, the Supervisory Board. The relevant body shall be required to respond to any indication of potential retaliation against such persons or in connection with the Report.
2. A Whistleblower who has made a Report and whose personal data have been disclosed without justification, or who has experienced retaliation, discrimination, or any other form of unfair treatment, should immediately notify the Company's Management Board of the situation.

The same shall apply where such actions or conduct are experienced by a person assisting the Whistleblower or a person associated with the Whistleblower. Where the Report concerns a member of the Management Board, the notification shall be made to the Supervisory Board instead. The Management Board or, as applicable, the Supervisory Board shall take appropriate measures to protect the Whistleblower and any person assisting in the submission of the Report or associated with the Whistleblower (provided that such person is employed by the Company or otherwise performs work for the Company), provided that the allegations set out in the notification are substantiated.

VII. EXTERNAL REPORTS

§ 24

The Company encourages Whistleblowers to **report information concerning a Breach to the Company in the first instance, in accordance with the procedure set out in this Procedure**, particularly with respect to the types of Breaches referred to in § 4(3) of the Procedure. However, a Reporting Person may, in any case, make an External Report directly to a Public Authority or the Central Authority without first making an Internal Report, in particular where:

- within the deadline for providing feedback referred to in § 14, the Company does not undertake follow-up actions or does not transmit feedback to the Reporting Person, or
- the Reporting Person has reasonable grounds to believe that the breach of law may constitute a direct or obvious threat to the public interest, in particular there is a risk of irreversible damage, or
- making an Internal Report would expose the Reporting Person to retaliatory actions, or
- in the event of making an Internal Report, there is a low probability of effective counteracting the breach of law by the Company due to special circumstances of the case, such as the possibility of concealing or destroying evidence or the possibility of the existence of collusion

between the Company and the perpetrator of the Breach or the Company's participation in the Breach.

§ 25

1. External Reports are accepted by the Central Authority or by a Public Authority in accordance with the reporting reception procedure developed by that authority.
2. The Central Authority (Commissioner for Human Rights) accepts External Reports in matters concerning breaches of law in areas referred to in the Act (and respectively: in § 4 paragraph 2 of the Procedure).
3. The President of the Office of Competition and Consumer Protection, as a competent Public Authority, accepts External Reports in matters of breaches of competition rules and consumer protection. Other Public Authorities accept External Reports in matters of breaches regarding operation of a given Public Authority.
4. External Reports can be anonymous or allow for the identification of the reporting person. For the purpose of effectively undertaking follow-up actions and transmitting information about undertaken follow-up actions in an external report, the reporting person provides a correspondence address or e-mail address. The administrator of personal data provided in an External Report is the Central Authority or Public Authority accepting the External Report.
5. An External Report can be made orally, i.e.:
 - by telephone via a recorded hotline, or
 - at the request of the reporting person—during a direct meeting organized at the seat of the authority accepting the External Report on a designated date, no longer than 7 days from the day of submitting the request,

or can be made in paper or electronic form, i.e.:

- in paper form—to the correspondence address indicated by the reporting authority;

- in electronic form—to the e-mail address indicated by the reporting authority.

6. Handling of External Reports can take place in the ICT system of the Central Authority or Public Authority. In such a case, the External Report is submitted in the form of an electronic document, in accordance with the template made available on the website by the Central Authority or Public Authority.
7. The Central Authority or Public Authority accepting the External Report confirms its acceptance to the reporting person to the contact address immediately, no later however than within 7 working days from the day of receiving the report, provided that the reporting person has provided a contact address.
8. Communication means accepted by the Central Authority or Public Authority for the purposes of receiving External Reports:
 1. are independent of the communication channels used by the relevant authority in the course of its ordinary activities;
 2. ensure confidentiality and integrity of data, including their safeguarding against reading by unauthorized persons.

§ 26

1. The Central Authority shall determine the detailed procedure for verifying and examining an External Report, taking into account the relevant provisions of Chapter 4 of the Act.
2. The Public Authority shall determine the detailed procedure for verifying and examining an External Report, taking into account the relevant provisions of Chapter 4 of the Act.
3. The Central Authority and Public Authority place on their websites, in a manner understandable to reporting persons, information on:
 1. contact details for submitting an External Report, including, in particular,

- a postal address, email address, and telephone hotline number;
 - 2. conditions for qualifying the reporting person to be covered by protection;
 - 3. procedure mode applicable in the event of an External Report;
 - 4. confidentiality rules applicable to External Reports, including information related to personal data processing;
 - 5. character of follow-up actions undertaken in connection with the External Report;
 - 6. legal protection measures and procedures serving protection against retaliatory actions and availability of confidential advice for persons considering making an External Report;
 - 7. conditions under which the reporting person is protected against liability for breach of confidentiality.
4. The Public Authority shall also publish on its website the contact details of the Central Authority (the Commissioner for Human Rights).

VIII. REGISTER OF BREACH REPORTS

§ 27

- 1. Based on Reports received and information provided by the Commission, the Management Board, or the Supervisory Board, the Investor Relations Consultant shall make the relevant entries in the Register of Breach Reports and shall maintain and regularly update the Register.
- 2. The Register of Breach Reports is maintained in electronic form; documentation related to a given Breach is recorded and maintained in paper or electronic form.
- 3. The Register of Breach Reports should contain at least the following elements:
 - 1. date of receipt of the Report and/or reception of the Report by the Recipient together with the date of

- transmitting the confirmation of acceptance of the Report to the Reporting Person, if possible (in accordance with the provisions of § 10 of the Procedure);
 - 2. report number;
 - 3. subject of the Breach;
 - 4. insofar as it results from the Report and the nature of the case: personal data of the Reporting Person (including contact address) and/or personal data of the person or persons to whom the reported Abuse relates, taking into account the provisions of paragraph 5 of this paragraph of the Procedure; provisions of § 18 paragraph 3 first sentence, paragraph 4 and paragraph 5 apply;
 - 5. personal data of Commission members appointed to examine the Report in accordance with relevant provisions of § 12 of the Procedure;
 - 6. basic information on the subject matter of the Report, together with documentation of the process of analyzing and examining the Report (including documents, minutes, notes, etc.);
 - 7. the grounds for initiating or refusing to initiate investigatory proceedings;
 - 8. a description of how the Breach Report was examined, including, in particular, information on decisions taken and follow-up and preventive measures implemented;
 - 9. date of closing the case.
4. The Register of Breach Reports shall be updated on an ongoing basis whenever a Report is received or new information comes to light in the course of the investigatory proceedings.
5. The Register of Breach Reports shall be maintained in accordance with applicable data

protection requirements, including, in particular, Regulation (EU) 2016/679 (GDPR), and with due regard to the confidentiality of the information contained therein. The standards set out in § 18 of this Procedure shall apply accordingly.

6. Personal data recorded in the Register of Breach Reports and processed in connection with the receipt of a Report shall be retained by the Company for no longer than **three years** from the date on which the Report was received.

§ 28

1. The Commission, Management Board, or Supervisory Board may at any time turn to the Investor Relations Consultant for additional information regarding reports disclosed in the Register of Breach Reports.
2. The Supervisory Board may at any time submit a request to the Management Board to provide information on the current status of reports and the stage of their processing.

IX. PERSONAL DATA PROCESSING

§ 29

1. The administrator of the personal data of the Whistleblower and the personal data of the persons to whom the Report relates, provided by the Whistleblower within the framework of the Report, including data encompassed by the Register of Breach Reports, is the Company, i.e., Rainbow Tours Spółka Akcyjna with its registered office in Łódź, address: ul. Piotrkowska 270, 90-361 Łódź, e-mail address: sekretariat@r.pl, telephone number: +48 42 680 3880, entered into the Register of Entrepreneurs of the National Court Register kept by the District Court for Łódź-Śródmieście in Łódź, XX Commercial Division of the National Court Register, KRS number: 0000178650, NIP number: 7251868136, REGON number: 473190014.
2. The Company, as the data controller, has appointed a Data Protection Officer who can be contacted via e-mail at the e-mail address: rodo@r.pl.

§ 30

1. The legal basis for processing the personal data of the Whistleblower and the personal data provided by the Whistleblower within the framework of the Report constitutes:

1. **Article 6 paragraph 1 letter c) of the GDPR**, i.e., fulfillment of a legal obligation incumbent on the Company (data controller) resulting from:

- Article 97d of the Act on Public Offering,
- the Act,
- Regulation 596/2014 (MAR);

2. **Article 6 paragraph 1 letter f) of the GDPR**, i.e., purposes resulting from legitimate interests pursued by the Company (data controller) or by a third party (e.g., Client or Contractor, Employee, etc.), to which belong:

- protection of the interests of the Company or a third party through the prevention of potential damage and detection of potential or actual dangers and threats to the broadly understood interest of the Company or third parties which otherwise would remain undetected,
- other interests threatened by a Breach, including in particular threatened by one of the Breaches indicated in § 4 paragraph 2 or paragraph 3 of the Procedure.

2. Personal data are processed for the following purposes:

1. reporting potential or occurred Breaches,
2. verification of the merits of reported potential or occurred Breaches,
3. communicating with the Whistleblower,

4. maintaining the Register of Breach Reports.
3. Personal data will not be subject to entirely automated processing, including profiling.
4. On the basis of relevant provisions of the Act, the Company, after receiving a Report, may, for the purpose of verifying the Report and taking follow-up actions, **collect and process the personal data of the person to whom the Report relates, even without their consent.** The provision of Article 14 paragraph 2 letter f) of the GDPR (i.e., concerning the obligation to indicate the source of origin of personal data) does not apply, unless the Reporting Person acted in a situation of not possessing reasonable grounds to believe that the information on the Breach constituting the subject of the Report was true at the time of making the Report and that such information constituted information on a Breach.

§ 31

Personal data relating to the person concerned by a Breach Report may include special categories of personal data within the meaning of the GDPR and the Company's applicable data protection policies. Such data may include, for example, information provided by the Whistleblower concerning the activities or conduct of the person concerned, including their professional relationships and economic or social behavior.

§ 32

1. Personal data may be disclosed to entities processing personal data on behalf of the data controller, as well as to public authorities and other entities legally authorized to access such data, including courts, law enforcement authorities, and state institutions such as the Polish Financial Supervision Authority (Komisja Nadzoru Finansowego), where they make a request based on an appropriate legal basis.
2. Personal data may also be disclosed within the Capital Group where such disclosure is necessary to conduct an investigation under the Procedure.

§ 33

1. A person to whom personal data relate has the right to request from the Company, as the data controller:
 - access to their personal data (Article 15 of the GDPR),
 - request for rectification of their personal data which are incorrect and completion of incomplete personal data (Article 16 of the GDPR),
 - request for restriction of processing of their personal data in situations indicated in Article 18 of the GDPR,
 - lodging a complaint with a supervisory authority dealing with personal data protection, i.e., the President of the Personal Data Protection Office
2. Pursuant to Article 21(1) of the GDPR, a data subject has the right to object, at any time and on grounds relating to their particular situation, to the processing of personal data concerning them where such processing is based on Article 6(1)(f) of the GDPR, including profiling based on that provision. In such a case, the controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or unless the processing is necessary for the establishment, exercise, or defense of legal claims.
3. A person to whom personal data relate does not have the right to:
 - request the erasure of their personal data, subject to the exception set out in Article 17(3)(b) of the GDPR;
 - exercise the right to data portability, as the conditions set out in Article 20(1) of the GDPR are not met.

§ 34

1. Personal data processed in connection with the receipt of a Report shall be retained by the

Company for no longer than three years from the date on which the Report was received.

2. Subject to paragraph 1 of this section of the Procedure, the retention period for the personal data of the Whistleblower or the person concerned by the Report shall depend on the purpose for which the data are processed. Accordingly, personal data shall be processed for as long as required under applicable laws that oblige the Company to retain or otherwise process such data for a specified period.
3. Subject to paragraph 1 of this section of the Procedure, the personal data of the Whistleblower or the person concerned by the Report shall be retained for as long as necessary to conduct an appropriate investigation in accordance with the procedures set out in the Procedure. Personal data shall not be retained for longer than is necessary in light of the purpose for which they are processed.
4. If the Report is found to be unsubstantiated and the allegations contained therein are dismissed, the Company shall promptly delete from its systems the personal data contained in the Report. Other information contained in the Report, together with information concerning the follow-up actions taken, shall be retained in the Company's systems for three years, calculated from the first day of the year following the year in which the Report was made.
5. If the personal data provided by the Whistleblower are not relevant to the allegations contained in the Report (e.g., information concerning the Whistleblower's family or personal circumstances), such data shall not be further processed and shall be promptly deleted or anonymized.

X. FINAL PROVISIONS

§ 35

1. This Procedure has been established after consultation with the representatives of the Company's Employees. The Procedure and its amendments are communicated to Employees

in the standard manner adopted in the Company.

2. The Procedure enters into force upon the expiry of **7 days** from the day of communicating the Procedure to its addressees.
3. The Company (as an employer within the meaning of the Labour Code) provides all job applicants and the aforementioned individuals with information on how to access and review the whistleblower procedure at the very beginning of recruitment or contract negotiations.
 - persons employed in the Company on the basis of a civil law contract (e.g., specific task contract or mandate contract),
 - sole proprietors conducting business personally in relation to the Company (including those operating under "B2B" cooperation agreements),
 - persons serving apprenticeships, interns, or volunteers in the Company,
 - members of the Management Board or Supervisory Board. Additionally, the Company ensures that all job applicants and the aforementioned individuals are informed about the availability of the reporting procedure at the very beginning of the recruitment process or contract negotiations. members of the Management Board or Supervisory Board. Additionally, the Company ensures that all job applicants and the aforementioned individuals are informed about the availability of the reporting procedure at the very beginning of the recruitment process or contract negotiations.
4. Employees and other individuals mentioned in paragraph 3, second sentence above, are required to thoroughly review the Procedure and comply with its provisions.

5. Failure to follow the rules set out in the Procedure constitutes a breach of employee duties for those subject to the Labour Code and may result in disciplinary action under applicable employment regulations.
6. Detailed criminal provisions—including penalties such as fines, restriction of liberty, or imprisonment—concerning offenses related to:
 - preventing or substantially hindering the making of an Internal Report or External Report,
 - undertaking retaliatory actions against a person who drew up an Internal Report or External Report and a person assisting in the report or a person associated with the Whistleblower,
 - violating the obligation to maintain the confidentiality of the identity of a person who drew up an Internal Report or External Report,
 - reporting false information through an Internal or External Report—are set forth in the provisions of the Act.

§ 36

1. This Procedure is an internal document and must not be disclosed or made available to unauthorized persons in any form, unless authorized, required by applicable laws or regulations, mandated by a court order or a competent judicial, governmental, banking, tax, or other regulatory body (in particular the Polish Financial Supervision Authority), or required by applicable stock exchange rules.
2. Any matters not covered by this Procedure shall be governed by the relevant laws and legal acts pertaining to the matters addressed herein.

§ 37

1. The Management Board is responsible for ensuring the adequacy and effectiveness of this Procedure.

2. Amendments to the Procedure may be made by a resolution of the Management Board.

(Signed by):

Maciej Szczechura – President of the Management Board

Piotr Burwicz – Vice-President of the Management Board

Jakub Puchałka – Vice-President of the Management Board

Aleksandra Piwko-Susik – Member of the Management Board