4IG Information Technology Ltd.

WHISTLEBLOWING AND WHISTLEBLOWER PROTECTION POLICY

Identifier	Version	Effective	Related regulation	Limited application
COM4_4IGIT	1.0	02.01.2025	Anti-corruption Compliance Function Policy Rules of Procedure of the Ethics Committee	Public

RELEASE

Regulatory function	Name	Operation	Position	Date of DOQ approval/ Signature
Process owner	Melinda Kurucz	Group Compliance	Compliance specialist	
Signatory for compliance	Eszter Katalin Forrai	Group Quality Management and Regulation	Group Quality Management and Regulation Director	
Signatory for compliance	Melinda Kurucz	Group Compliance	Compliance specialist	
Signatory for compliance	dr. Eva Szántó	Group Legal	Head of Legal Affairs	
Signatory for compliance	dr. Judit Lerch	IT Business Portfolio Management	Director of IT Business Portfolio Management	
Signatory for compliance	Richárd Somodari	Information security	Information Security Representative	
Approver	Gábor Radó	Chief Executive Officer	Chief Executive Officer	

DOCUMENT HISTORY

Version	Date of entry into force	Short description of modification
1.0	02.01.2025.	Issue of new rules

Contents

1. SCOPE AND RESPONSIBILITIES

1.1 SCOPE

1.1.1 Personal scope

The scope of this Whistleblowing and Whistleblower Protection Policy (hereinafter: the "Policy") extends to 4iG Information Technology Ltd. (hereinafter: "our Company" or "we") and to all its employees, executive officers, and the persons concerned by the report.

1.1.2 Term

This Policy enters into force upon its adoption and promulgation by the CEO and remains in effect until revoked

1.1.3 Objective scope

The scope of this Policy extends to:

- any report concerning information about acts, omissions, or other forms of misconduct involving our company that are unlawful or suspected to be unlawful (hereinafter: "violation of rules"), including in particular:
  - conduct that violates or is suspected of violating applicable laws (including European Union regulations);
  - acts or omissions that are suspected of violating the requirements and fundamental ethical expectations set out in our company's Code of Ethics and Business Conduct, Code of Ethics for Business Partners, and other policies, as well as other forms of misconduct related to internal policies,

submitted in relation to our company.

2. STRATEGY AND GOALS

We are committed to establishing and continuously developing ethical operations and a value-driven corporate culture that comply with applicable legal requirements (including European Union regulations) and align with our company's Code of Conduct, Code of Ethics for Business Partners, and internal policies.

We are convinced that a properly designed and implemented compliance program—which includes an anti-bribery management system based on the MSZ ISO 37001:2019 standard—provides an appropriate framework for this. An integral part of the operation of our compliance program and anti-bribery management system is ensuring that any potential violations of rules occurring within our company—including, in particular but not exclusively, acts of corruption, fraud, and activities or omissions related to money laundering and the financing of terrorism—do not remain undetected.

We are convinced that individuals—whether employees, contractual partners, or clients—who are the first to detect a violation of rules or an imminent risk thereof play a pivotal role in uncovering and preventing such violations. Therefore, we attach great importance to facilitating the swift and direct transmission of relevant information and any potential evidence to the person with the competence and authority to investigate the matter.

To ensure this—and in accordance with the relevant provisions of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, as well as the implementing Act XXV of 2023 on Complaints, Public Interest Disclosures, and Rules Related to the Reporting of Misconduct (hereinafter: the "Complaints Act")—we operate a system for reporting misconduct (a so-called "whistleblowing" system).

Reports concerning the violations defined in Section 1.1.3 of this policy may be submitted through the whistleblowing system.

The reporting channel we provide (the so-called Ethics and Compliance Line; see Section 4.2 for details) serves as a confidential forum for handling reports, facilitating the detection and resolution of violations (e.g., misconduct, ethical breaches, and legal violations). This helps strengthen a corporate culture based on trust and fair conduct while preserving our company's good reputation.

However, individuals wishing to report suspected violations may be deterred from voicing their concerns or suspicions by a fear of retaliation. In light of this, we have designed our whistleblowing channel so that reports are investigated by an independent and impartial control function—the Compliance function (hereinafter: "Compliance")—or, in cases where the Compliance function itself is implicated, by Group Internal Audit.

Access to the content of reports is restricted to the Compliance function, Compliance Officers, and—to the extent necessary for the investigation—those individuals participating in the inquiry. Persons implicated in a report may access information regarding it only to the extent that such access does not reveal the identity of the whistleblower. Furthermore, we provide the option to submit completely anonymous reports and have implemented measures to protect whistleblowers. To achieve the aforementioned objectives, this Policy outlines the operating principles and process of the whistleblowing system we operate, the persons and entities responsible for handling reports, and the safeguards ensuring the protection of whistleblowers.

3. VIOLATION OF RULES AS UNACCEPTABLE CONDUCT

In accordance with the material scope of this Policy (Section 1.1.3), any act, omission, or other form of misconduct constitutes unacceptable conduct if it:

- may violate or is alleged to violate any applicable law or regulation (including European Union norms);
- presumably violates the requirements and fundamental ethical expectations set forth in our Company's Code of Ethics and Business Conduct, the Business Partner Code of Ethics, and our other policies, or may conflict with our internal regulations.

We consider such unacceptable conduct to include, in particular, discrimination, corruption, fraud, acts related to money laundering, as well as activities involving unfair market practices and the restriction of competition; our company takes rigorous action against such conduct in accordance with its internal regulations (specifically the Code of Ethics and Business Conduct, the Code of Ethics for Business Partners, and the Anti-Corruption and Anti-Bribery Policy).

Such unacceptable conduct violates—or has the potential to violate—the legitimate interests or reputations of our company, the entire 4iG Group, and 4iG Group employees; therefore, we attach great importance to taking action against illegal, unfair, or unethical behavior.

4. WHISTLEBLOWER REPORTS

4.1 PERSON AUTHORIZED TO FILE REPORTS

Any person who has knowledge of a potential violation of rules (hereinafter: "whistleblower") may submit a report through the whistleblowing system. Thus, reports may be submitted in particular by:

- an employee of our company;
- a former employee whose employment relationship with our company has terminated;

a) a natural person intending to establish an employment relationship with us, where the procedure for establishing such a relationship has already commenced;

b) a sole proprietor or sole proprietorship that has a contractual relationship with us, is participating in a procedure to establish such a relationship, or previously had a contractual relationship with us;

c) a person holding an ownership interest in our company, a member of the board of directors or supervisory board, an employee authorized to represent the company, or a person for whom the procedure to establish such a relationship or contractual connection has already commenced or whose such relationship or contractual connection with us has already terminated;

d) a contractor, subcontractor, or supplier who is participating in a procedure to establish a contractual relationship with us, has a contractual relationship with us, or previously had a contractual relationship with us, as well as any other person acting under the supervision and direction of a person commissioned by us;
e) an intern or volunteer performing activities at our company, or a person for whom the procedure to establish an internship or volunteer relationship has commenced or has terminated.

4.2. REPORTING PROCEDURE – ETHICS AND COMPLIANCE CHANEL

In the event of violation of company policies or suspicion thereof, reports may be submitted to Compliance through the following channels, collectively referred to as the Ethics and Compliance Chanel:

1) via the channel operated on the 4iG Information Technology Ltd. website (direct contact: 4iG Informatikai Zrt.);
2) via the email address compliance-itsi@4ig.hu;
3) in person with any Compliance Officer within the Compliance function;
4) by mail, in a letter addressed to "4iG Information Technology Ltd. Compliance" (to the postal address: 1037 Budapest, Montevideo utca 2/C).

4iG Plc. and 4iG Information Technology Ltd independently investigate reports concerning the Company that it receives, whereas reports submitted via the whistleblowing channel operated by us are investigated by the Company's Compliance Officer, in accordance with the provisions of Section 4.6.3.2.

Any indication of conduct potentially violating rules or standards, submitted to the person authorized to receive such information, qualifies as a report. The report must contain a sufficient amount of information and detail to enable the investigation to commence.

Employees of the Company are required to submit a report to the Compliance function whenever they encounter unacceptable conduct.

Reports submitted via the aforementioned channels are received by Compliance; the identity of the reporting person (unless the report is anonymous) and their contact details are known only to the Compliance Officer handling the matter. Employees from other organizational units may access such data only to the extent necessary for their contribution to the investigation. In cases involving proceedings by the Ethics Committee, members of the Ethics Committee may also access the reporting person's personal data. If a report is not received directly by the Compliance function, it must be forwarded to Compliance immediately and confidentially, regardless of the channel used or the type of report (anonymous or non-anonymous).

If, in the opinion of the Compliance, the conduct described in the whistleblower report does not constitute unacceptable conduct subject to investigation under this Policy, but the investigation of such conduct falls within the powers of an organisational unit or member company within 4iG Group, they shall forward it directly to the head of the organisational unit or member company with the relevant powers, together with notifying the whistleblower.

4.3. LANGUAGE OF THE WHISTLEBLOWER REPORT

Whistleblower reports can be submitted through the channels specified in point 4.1 in Hungarian and English.

4.4. ENABLING ANONYMOUS WHISTLEBLOWING

Anonymous whistleblowing is also possible. In the case of anonymous whistleblowing, the 4iG Group does not seek to identify the whistleblower in any way; however, for an efficient investigation, the organisation prefers that the whistleblower provides contact details. The resulting bilateral communication facilitates the investigation of the whistleblower report and enables the whistleblower to provide additional information and to monitor the process and results of the procedure while their personal protection can be ensured more easily.

The absence of contact details is not an obstacle to the procedure, but it is not possible to supply missing information and inform the whistleblower.

4.5. DATA PROCESSED

Whistleblower reports may also be submitted by providing only the minimum information required, but please provide the following information if possible:

1) the name, business address or home address, telephone number or e-mail address (if any) of the whistleblower (optional in the case of an anonymous whistleblower report);
2) the fact that the whistleblower is a whistleblower (employment relationship, agency, contractor or other legal relationship, legitimate interest in remedying or terminating the conduct which is the subject of the whistleblower report)
3) if known to the whistleblower, the name and position of the person(s) affected by the whistleblower report, and their relationship with the 4iG Group;
4) a description of the suspected unacceptable conduct and all information necessary for assessing the case;
5) evidence related to the case which supports that an ethical abuse has been committed.

In the case of a whistleblower report by e-mail, the whistleblower may attach documents that may provide additional clue during the investigation. In all cases, the data provided will be treated in the strictest confidence, in accordance with the relevant data protection regulations. The Privacy Policy and Data Processing Notice provides guidance on data processing.

4.6. MANAGEMENT OF WHISTLEBLOWER REPORTS

4.6.1. Written Report

A report is considered to have been made in writing if it is:

- sent by post in a letter addressed to "4iG Information Technology Ltd. Compliance";
- sent to the email address compliance-itsi@4ig.hu;
- or submitted via the online channel available at https://compliance.4ig.hu/etikai-es-compliance-bejelentes/

If the whistleblower has provided contact details, the Compliance Officer will acknowledge receipt of the report within 7 days of receiving it. In the acknowledgment, the Compliance Officer provides the whistleblower with general information regarding the procedure for investigating the report and the rules governing data processing.
Furthermore, we make clear and easily accessible information available regarding our whistleblowing system, the procedure related to reports, and the systems and procedures available under the Complaints Act:

- to our employees on our internal Compliance page;
- on the website compliance.4ig.hu.

4.6.2. Oral Report

Reports may also be made orally. Reports made in person to the Compliance Officer are considered oral reports. The Compliance Officer prepares a record of the oral report.

In the case of an oral report, prior to the report being made, the Compliance Officer:

- draws the whistleblower's attention to the consequences of making a report in bad faith,
- informs them of the rules governing the investigation of the report, and
- informs them that the whistleblower's identity will be treated confidentially at all stages of the investigation, provided the whistleblower supplies the data necessary for their identification,
- provides information on where the data processing notice can be accessed.

When documenting the personal report, the Compliance Officer prepares a complete and accurate record.

The Compliance Officer prepares a record of the oral report in a durable and retrievable format, puts it in writing, and provides it to the whistleblower for review and correction, while also ensuring the opportunity for acceptance via signature.

Following the making or receipt of the report, the Compliance Officer examines the report to determine whether it falls within the scope of this Policy and whether there is any conflict of interest concerning the Compliance Officer and the compliance function.

4.7. REVIEW OF THE REPORT

4.7.1. Reports Concerning 4iG Information Technology Ltd.

If a report concerning our company is received by the Ethics and Compliance Chanel, the Compliance Officer will investigate the contents of the report as soon as possible after its receipt—but no later than 30 days from the date of receipt—and take the necessary measures.

In particularly justified cases, the Compliance Officer may extend the investigation deadline once—by a maximum of two additional months—while simultaneously notifying the whistleblower. The whistleblower must be informed of the extension of the investigation within 30 days of the report being filed.

4.7.2. Reports addressed to 4iG Plc. and concerning our company

If the whistleblower submits their report directly to 4iG Plc. (as the company responsible for group-level compliance within the 4iG Group) via 4iG Plc.'s Ethics and Compliance Hotline, the report shall be investigated by 4iG Plc.'s Compliance Officer in accordance with the whistleblowing and whistleblower protection policy issued by 4iG Plc. (containing similar provisions), and 4iG Plc.'s Compliance Officer shall maintain contact with the whistleblower.

If the report is received through the whistleblowing system operated by us, then:

1) the employee performing the Compliance function at the company shall inform the Group Compliance Head of the report within 3 working days of its receipt, and shall also indicate to the Group Compliance Head if the investigation of the report may be omitted pursuant to points 6.1 or 6.2;

2) the Group Compliance Head shall subsequently review the report on a priority basis and determine the direction of the investigation to be conducted by the Compliance Officer;

3) the Compliance Officer shall investigate the report in accordance with the guidance of the Group Compliance Head and take the necessary measures;

4) the Compliance Officer shall inform the Group Compliance Head of the specific measures taken or planned—concurrently with informing the whistleblower—and, following the conclusion of the investigation, shall prepare a report on the investigation for the Group Compliance Head;

5) upon receipt of the report, the Group Compliance Officer decides whether the report can be closed under their own authority or whether it is necessary to initiate proceedings by the Ethics Committee, and decides on the commencement of such proceedings;

6) the Compliance Officer informs the whistleblower of the commencement of the Ethics Committee's proceedings and of the conclusion of the investigation into the report.

4.8. COMMUNICATION, SUBMISSION OF MISSING INFORMATION

Except in the case of anonymous reports, the Compliance Officer maintains contact with the whistleblower during the investigation of the report. As part of this communication, the Compliance Officer may return the report to the whistleblower—specifying any deficiencies and setting a short deadline (maximum of 5 working days) for rectification.

In this context, the Compliance Officer may request that the report be supplemented or clarified, that the facts of the case be elucidated, and that additional information be provided.

If the whistleblower fails to provide the information requested by the Compliance Officer or states that they possess no further information—and provided the Compliance Officer does not decide to forgo the investigation—the Compliance Officer shall proceed with the investigation based on the information available.

During the investigation, the Compliance Officer informs the whistleblower of any measures taken or planned, as well as the outcome of the investigation.

4.9. NON-PERMISSIBLE WHISTLEBLOWER REPORTS

The Compliance Officer may decide not to investigate the report if:

a) the whistleblower has submitted the report repeatedly with the same content;

b) any infringement of the rights of the person concerned by the report—resulting from the investigation—would be disproportionate to the public interest or the compelling private interest at stake.

In the event of a decision not to investigate, the Compliance Officer shall inform the whistleblower in writing (including via e-mail) of the decision and the reasons for it, provided the report was not submitted anonymously.

5. BASIC PRINCIPLES OF MANAGING WHISTLE-BLOWER REPORTS

5.1. PROTECTION OF WHISTLEBLOWERS

The protection of whistleblowers is of paramount importance to us; therefore, we ensure that the whistleblower is not subjected to any form of reprisal, discrimination, retaliation, or other unfair treatment (collectively: "adverse measure").

Accordingly, any adverse measure taken against the whistleblower as a result of making a report is prohibited; this includes the protection of persons holding a legal relationship defined in Section 4.1, as well as persons whose legal relationship defined in Section 4.1 has terminated or for whom the process of establishing such a relationship has already commenced.

Any and all forms of retaliation constitute an adverse measure, particularly:
1. termination of a mandate, contractor, or lease relationship;
2. causing harm, including damage to a person's reputation—particularly on social media—or financial loss, including the loss of business opportunities and loss of revenue;
3. premature termination or cancellation of a contract for goods or services;
4. revocation of a license or permit;
5. blacklisting based on an informal or formal sector- or industry-wide agreement, which may result in the person being unable to find future employment within that sector or industry;
6. in the case of employees, the following may also constitute such measures:
a. discrimination, suspension, layoff, collective redundancy, dismissal, or equivalent measures;
b. demotion or denial of promotion;
c. reassignment of job duties, change of workplace, reduction in wages, or alteration of working hours;
d. denial of training;
e. negative performance appraisal or employment reference;
f. imposition of any disciplinary or other adverse employment-related measure, reprimand, or sanction, including wage deductions;
g. coercion, intimidation, harassment, or ostracism;
h. discrimination, or adverse or unfair treatment; i. failure to convert a fixed-term employment contract into an indefinite-term employment contract, where the employee had a legitimate expectation of being offered indefinite-term employment;
j. failure to renew a fixed-term employment contract or the premature termination thereof;
k. causing damage, including infringement of a person's reputation—particularly on social media—or financial loss, including the loss of business opportunities and loss of revenue;
l. mandating a medical fitness examination.

A whistleblower shall not suffer any disadvantage even if the report—made in good faith or based on a reasonable conviction—proves to be unfounded during the investigation (unless the whistleblower themselves participated in the conduct described in the report).

Any detrimental measure taken against the whistleblower—or against an entity owned by 4iG Plc. or an entity with which the whistleblower has an employment, engagement, or other contractual relationship—as a result of the lawful submission of the report shall be deemed unlawful.

If a whistleblower acting in good faith demonstrably suffers a disadvantage, this shall entail employment-law consequences for the person responsible for causing said disadvantage. The member company of the 4iG Group that caused the disadvantage—including our company—shall be liable to the whistleblower for the proven detriment.

The whistleblower is entitled to protection even if, for the purpose of making a lawful report, they disclose a secret protected by law under any EU legislation or the national legislation transposing it (as listed in Annexes 1 and 2 of the Complaints Act), provided such disclosure was necessary to uncover the circumstances addressed in the report.

5.2. CONFINDENTAL INFORMATION MANAGEMENT

Our company processes personal data in accordance with the provisions of Regulation (EU) 2016/679 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 (hereinafter: "GDPR"), as well as Act CXII of 2011 on the Right of Informational Self-Determination and on the Freedom of Information (hereinafter: "Infotv.").

The Compliance Officer ensures that the identity of a person making a non-anonymous report is not disclosed to anyone other than those investigating the report. The personal data of the whistleblower and all persons involved in the report must be handled in accordance with applicable data protection laws, and the content of reports must be treated confidentially in every instance and at all stages of the investigation.
The Compliance Officer may share the content of the report and information concerning the person involved in the report with other organizational units or employees of the company—with the exception of the Ethics Committee—only to the extent strictly necessary for conducting the investigation.

Within the framework of the whistleblowing system established by this Policy, the Compliance Officer processes the data of the whistleblower(s), the person(s) concerned by the report, and any person(s) possessing substantive information regarding the contents of the report for the purposes of conducting the investigation or implementing measures recommended as a result thereof, initiating and conducting proceedings before the Ethics Committee, and enabling the Ethics Committee to reach a decision.

The personal data of the whistleblower and the persons concerned by the report may only be disclosed with their consent, and such personal data may only be transferred to—or must be transferred to—an authority competent to conduct the relevant proceedings. Any disclosure made in violation of these rules constitutes a breach of this Policy and may entail employment-related consequences or lead to regulatory sanctions.

If the report concerns a natural person, and that person submits a data subject request exercising their right of access under the GDPR, the whistleblower's personal data must not be disclosed to them during the fulfillment of that request.

5.3. REQUIREMENT OF GOOD FAITH

The report must be made in good faith regarding the circumstances known to the reporting person. A report proven to be made in bad faith, intentional deception, or the provision of false information entails legal consequences.

If it becomes evident that the report was made in bad faith by providing false data or information, and
a) circumstances arise indicating the commission of a criminal offense or an administrative offense, our company shall transfer the whistleblower's personal data to the body or person authorized to conduct the proceedings;

b) the offense qualifies as one prosecutable only upon a private complaint, our company may transfer the data to the body authorized to conduct the proceedings subject to the whistleblower's consent;

c) there are reasonable grounds to believe that the whistleblower has caused unlawful damage or other legal injury to another party, our company shall transfer their personal data upon the request of the body or person authorized to initiate or conduct proceedings

5.4. ENSURING A FAIR PROCESS

We ensure a fair, independent, and professional process. In every instance, the procedure is conducted in accordance with the spirit of our company's Code of Ethics and the provisions of this Policy, regardless of the positions or identities of the whistleblower and the person(s) concerned by the report.

5.5. UNIFORM PROCEDURE FOR HANDLING REPORTS

Every report—regardless of the channel used to submit it, and whether made orally or in writing, anonymously or non-anonymously, or with or without providing the reporter's contact details—must be investigated objectively and comprehensively, taking into account all available data and in accordance with the principles detailed above.

6. INVESTIGATION

6.1 NON-PERMISSIBLE WHISTLEBLOWER REPORTS

The investigation of a report with the same subject as a previous report may be dispensed with. Furthermore, the Compliance Officer may decide not to conduct an investigation if the harm to the public interest or a compelling private interest is disproportionate to the restriction of the rights of the person concerned by the report resulting from the investigation

6.2. NON-INVESTIGATION OF WHISTLEBLOWER REPORTS

If, in the judgment of the Compliance Officer, the facts described in the report do not constitute a violation of rules, the Officer shall terminate the procedure and, where necessary and based on the nature of the report's contents, may initiate other proceedings. In such cases, the Compliance Officer shall inform the whistleblower that other proceedings are being initiated and that personal data related to the report will no longer be processed within the framework of the whistleblowing system but will be deleted.

The Compliance Officer shall inform the whistleblower, the Ethics Committee (and, where necessary, Group Internal Audit), as well as the person or organizational unit authorized to conduct control processes, regarding the termination of the procedure and any further measures taken or proceedings initiated. If the investigation into the misconduct concerning a company belonging to the 4iG Group was conducted by Group Compliance, the head of that company shall also be informed.

The Head of Group Compliance is required to inform the Ethics Committee within 15 days of the termination of a whistleblowing procedure in cases where the matter did not fall within the scope of this Policy. Based on this information, the Ethics Committee is entitled to disregard the Compliance decision and instruct the Compliance Officer to conduct the investigation.

6.3. INVESTIGATION OF WHISTLEBLOWER REPORTS

At the same time as sending a copy of this Policy, the Compliance shall inform the persons concerned by the report (persons whose act or omission gave rise to the whistleblower report or who have relevant information about the contents of the report) about the following:

1) the whistleblower report;
2) their rights regarding the protection of their personal data;
3) the principles relating to the processing of personal data;
4) their right to comment on the whistleblower report, also through their legal representative, and to substantiate their comments with evidence.

A fair and impartial procedure must be ensured, which means that persons involved in the investigation must be given an opportunity to comment on the allegations made and evidence presented against them. These should be made available to them without compromising the success of the investigation.

The person concerned by the whistleblower report must be informed that they may engage a legal representative and may substantiate their position with evidence.

In particular, the following investigative tools may be used to establish the facts:

- interview (hearing) with the persons involved in the whistleblower report personally or via telephone or video conferencing;
- requesting available documents and other information related to the case; or
- viewing locations relevant to the case.

The persons involved in the whistleblower report shall cooperate with Compliance and the Compliance Officer in charge of the report, provide the documents requested and state all facts of which they are aware and which may be relevant for the assessment of the case.

However, no one shall be required to make a statement or provide a document incriminating themselves or any of their relatives. The Compliance is obliged to inform the persons involved in the whistleblower report about this right in advance.

A specialized expert (e.g., an external consultant) may be involved in the investigation of the report, subject to compliance with applicable data protection regulations. An external expert may only be engaged if they do not currently have—and have not had at any time during the five years preceding the conclusion of the relevant engagement contract—a contractual, employment, or other legal relationship involving an obligation to perform work with the 4iG Group or any member thereof.

The information can only be provided later if immediate disclosure would jeopardise the investigation of the whistleblower report.

6.4. CONFLICT OF INTEREST

If the whistleblower report also affects the Compliance Officer, the whistleblower may report the matter to the Group Internal Control for an unbiased assessment. If a whistleblower report involving the Compliance Officer is submitted to Group Compliance, the Head of Group Compliance shall immediately forward the report to Group Internal Control.

If the whistleblower report does not affect the Compliance Officer, the Compliance decides at their sole discretion whether or not an internal investigation needs to be conducted. In order to prevent possible failure to report, the employer should clearly draw the attention of its employees to the obligation to report actual or potential conflicts of interest.

The whistleblower, any person affected by the whistleblower report, and any person from whom an impartial assessment of the case cannot be expected for other reasons shall not be involved in the investigation of the report and in the subsequent decision making.

6.5. THE INVESTIGATION PROCESS

The investigation of the whistleblower report shall be carried out by Compliance, or, if Compliance is involved, by the Group Internal Control (hereinafter: “investigator-in-charge”). Where the investigator-in-charge is Group Internal Control, Group Internal Control shall have the rights and obligations of Compliance and the Compliance Officer in charge under this Chapter.

Where justified by the nature of the case, the investigator-in-charge may involve other departments in the investigation.

Hearing

The Compliance Officer in charge may also hear the persons involved in the whistleblower report personally, by telephone or by video conferencing, subject to compliance with the following provisions.

- In addition to the person to be heard, persons designated by the person concerned, in particular their legal representative, may be present at the hearing as assisting persons at the request of the person to be heard.
- In addition to the person concerned, their superior exercising the employer's rights or their legal representative may be present at the hearing of the person subject to the report as an assistant at their request. The assistant may not make a statement on behalf of the interviewee but may ask the interviewee questions after the interviewer.
- At the hearing, all participants (witnesses, experts) must be informed of their rights to the protection of their personal data (name, position, any conclusion drawn from what has been said about the case). The personal data of the interviewee shall be kept confidential, unless the interviewee has expressly consented to its disclosure.

Minutes shall be made of the hearing which the interviewee can inspect. The interviewee is also entitled to initiate the correction or supplementation of the minutes sent to them. Minutes shall be made of the hearing at the whistleblower's request

Requesting documents and other information

The person involved in the whistleblower report must provide the Compliance with the documents and information requested by the Compliance within 5 days of the request. In the event that the requested person has not or has not fully provided the Compliance with the required documents or statements, the Compliance shall call upon the requested person to supplement any missing information and details. The person involved in the whistleblower report must comply with the request for missing information within 5 days.

Termination of the whistleblowing procedure

The Compliance will terminate the whistleblowing procedure if

- in the absence of evidence, no conduct violating the provisions of the Code of Ethics or the related internal regulations can be established and no result can be expected from further evidentiary proceedings;
- it is clear that the conduct under investigation does not conflict with the Code of Ethics or the related internal regulations;
- the contents of the whistleblower report do not constitute an ethical matter;
- it is clear that the whistleblower report was made in bad faith; or
- the conduct under investigation has already been legally assessed by an authority or court, or the Ethics Committee has already taken a position on it.

The Compliance is required to report to the Ethics Committee on the termination of the whistleblowing procedure within 15 days of the termination of the procedure. Based on the findings, the Ethics Committee is entitled to disregard the decision of the Compliance and instruct the Compliance to send the whistleblower report and its attachments to the Ethics Committee.

The Compliance shall inform the whistleblower and the persons involved in the whistleblower report in writing of the termination of the whistleblowing procedure.

Deciding on the matter at sole discretion

In minor or easy-to-judge matters, the Compliance may decide on the matter in their own competence.

The Compliance is entitled to make one of the following decisions:

a) establish that the conduct or omission under investigation has violated one or more provisions of the Code of Ethics or the related internal regulations;

b) establish that the conduct or omission under the ethical procedure has not violated the provisions of the Code of Ethics or the related internal regulations.

The Compliance is required to report on these matters and their outcome to the Ethics Committee within 15 days. Based on the findings, the Ethics Committee is entitled to disregard the decision of the Compliance and instruct the Compliance to send the whistleblower report and its attachments to the Ethics Committee, and decide on the matter in its own competence.

If the Compliance establishes that the conduct or omission under investigation has violated one or more provisions of the Code of Ethics or the related internal regulations, the following sanctions may be imposed:

1) For employees:
a) initiating a verbal warning at the person exercising the employer rights;
b) initiating a written warning at the person exercising the employer rights;
c) initiating disciplinary proceedings at the person exercising the employer rights;
d) initiating termination of the employment at the person exercising the employer rights.

2) In the case of other contractual relationships, initiating the amendment or termination of the contract with the contractor.

In the event that the conduct covered by the whistleblower report justifies the initiation of judicial or authority proceedings based on the findings of the investigation, the Compliance shall immediately inform the officer or department authorised to initiate such proceedings. If a criminal report seems to be justified, the report shall be made in consultation with the Director of Security as the head of the organisation in charge of official contacts in criminal matters.

If, in the opinion of the Compliance, the outcome of the whistleblowing procedure would result in a warning (written or oral), disciplinary action or termination of employment concerning the employee subject to the whistleblower report, the Compliance shall initiate internal procedures to take the relevant action with the persons and organisational units authorised to take such action.

The Compliance shall inform the whistleblower and the persons involved in the whistleblower report of the decision made in the case and the additional measures and proceedings initiated on the basis of this.

Initiating a decision by the Ethics Committee

If the Compliance does not decide on the matter within their competence based on the above, the Compliance shall request the Chair of the Ethics Committee to convene a meeting of the Ethics Committee or adopt a resolution without holding a meeting. At the same time, the Compliance shall submit to the Ethics Committee the whistleblower report and its attachments as well as the draft position to be issued by the Ethics Committee.

6.6. DECISION MAKING

The Ethics Committee of the 4iG Group is entitled to make a decision on the whistleblower reports after the investigation based on the contents of the investigation report. The Ethics Committee shall make a decision within a maximum of thirty (30) days of the completion of the investigation report. The Compliance shall inform the whistleblower of the decision of the Ethics Committee within fifteen (15) working days of the decision, but after informing the employee(s) concerned by the whistleblower report, provided that the whistleblower provides their name and contact details.

7. MONITORING THE FUNCTIONING OF THE WHISTLEBLOWING SYSTEM

The proper functioning of the whistleblowing system shall be reviewed at a frequency determined by the organisation, at least once a year, by an appropriate, competent and independent person designated for that purpose. The Group Compliance is required to report at least annually on the results of investigations and audits of whistleblower reports to the Board of Directors.

8. DATA ROTECTION

Information regarding the personal data of the whistleblower, the processing of personal data contained in the reports, and the rights of data subjects and available legal remedies in connection with such data processing is set out in the Data Processing Notice concerning whistleblower report.