WHISTLEBLOWING AND WHISTLEBLOWER PROTECTION PROCEDURE

1. Purpose and scope of the procedure

1.1 Purpose of the procedure

The purpose of this procedure is to establish the rules for receiving and processing reports of violations of the law and to ensure the protection of reporting persons at VIA 4 S.A. with its registered office in Mysłowice (the Company) in accordance with:
• the Whistleblower Protection Act of 14 June 2024, Journal of Laws 2024, item 928 (the Act),
• 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 (the Directive).

The procedure aims to prevent violations of the law, promote ethical conduct within the Company, and protect reporting persons against retaliatory measures.
Legal basis:
• Articles 1 and 2 of the Act,
• Article 1 of the Directive,
• Article 32 of the Constitution of the Republic of Poland (prohibition of discrimination),
• Articles 47 and 51 of the Constitution of the Republic of Poland (protection of privacy and personal data).

1.2 Scope of application

The procedure applies to all employees of the Company and members of the governing bodies, associates, contractors, suppliers and other entities working with the Company who have obtained information about irregularities in the course of their professional activities.
Legal basis:
• Article 4 of the Act (persons entitled to report),
• Article 2 of the Directive (personal scope),

2. Definitions

1. **Follow-up action** – an action taken by a legal entity or public authority to assess the truthfulness of the information contained in a report and to prevent the violation of the law covered by such report, in particular, by:
   - an investigation,
   - initiation of an inspection or administrative proceedings,
   - filing an indictment,
   - action taken to recover funds,
   - closure of the procedure carried out under the internal procedure for reporting violations of the law and undertaking follow-up action or under the procedure for receiving external reports and undertaking follow-up action.
   Legal basis: Article 2(1) the Act.
2. **Retaliatory measure (retaliation)** – a direct or indirect act or omission in a work-related context caused by a report or public disclosure that:
   - violates or may violate the rights of the Whistleblower,
   - causes or may cause unreasonable harm to the Whistleblower,

- includes the unwarranted initiation of proceedings against the Whistleblower.
Legal basis: Article 2(2) of the Act; Article 19 of the Directive.

3. **Information on violation of the law** – information, including a reasonable suspicion, regarding an existing or potential violation of the law, which:
(a) has occurred or is likely to occur in the Company in which the Whistleblower:
- participated in a recruitment process or other pre-contract negotiations,
- works or used to worked,
(b) has occurred or is likely to occur in another legal entity with which the Whistleblower:
- maintains or maintained contact in a work-related context,
(c) relates to an attempt to conceal such a violation of the law.
Legal basis: Article 2(3) of the Act.

4. **Feedback** – information provided to the Whistleblower on the follow-up action planned or taken and the reasons for such action.
Legal basis: Article 2(4) the Act.

5. **Work-related context** – past, present or future work-related activities based on:
- an employment relationship,
- another legal relationship forming the basis for the provision of work or services,
- a function performed within or for a legal entity,
- service performed within a legal entity,
where information on violation of the law has been obtained and there is a possibility of experiencing retaliation.
Legal basis: Article 2(5) of the Act.

6. **Public authority** – chief and central government administration bodies, territorial government administration bodies, bodies of local government units, other state bodies and other entities performing public administration tasks by virtue of law, competent to undertake follow-up action in the areas indicated in Article 3(1) of the Act.
Legal basis: Article 2(6) of the Act.

7. **Reported party** – a natural person, legal person or organisational unit without legal personality that is alleged to have violated the law that is the subject of the report or public disclosure.
Legal basis: Article 2(7) of the Act.

8. **Legal entity** – a natural person, legal person or organisational unit without legal personality conducting gainful, professional or other economic activity.
Legal basis: Article 2(10) of the Act.

9. **Whistleblower** – a natural person who reports or publicly discloses information on violation of the law obtained in a work-related context, including:
- an employee,
- a temporary worker,
- a person providing work on a basis other than an employment relationship, including under a civil law contract,
- an entrepreneur,
- a proxy,
- a shareholder,
- a member of a body of the Company or of an organisational unit without legal personality,

- a person who performs work under the supervision and management of a contractor, subcontractor or supplier,
- an intern,
- a volunteer,
- a trainee,
- an officer within the meaning of Article 1(1) of the Act of 18 February 1994 on retirement benefits for officers of the Police, Internal Security Agency, Intelligence Agency, Military Counterintelligence Service, Military Intelligence Service, Central Anti-Corruption Bureau, Border Guard, Marshal Guard, State Protection Service, State Fire Service, Customs and Tax Service, and Prison Service, as well as their families,
- a soldier within the meaning of Article 2(39) of the Act of 11 March 2022 on the defence of the Homeland.

Legal basis: Article 4 of the Act; Article 5 of the Directive.

10. **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC Personal Data Protection Act of 10 May 2018
(Journal of Laws of 2019, item 1781, as amended).

2.1 Violation of the law

Violation of the law means an act or omission that is contrary to legal provisions, in particular in the areas of:
• Public Procurement,
• Financial services, prevention of money laundering and terrorist financing,
• Product safety, environmental protection, public health, personal data, consumer protection, and other areas indicated in Article 3 of the Act.
Violation of the law also includes actions contrary to the organisation's internal regulations, which may lead to a violation of the public interest.
Legal basis:
• Article 3 of the Act (substantive scope of reports),
• Article 2(1) of the Directive (scope of violations of Union law),
• Article 7 of the Constitution of the Republic of Poland (principle of legalism – duty to act on the basis and within the boundaries of the law).

2.2 Report

A report means the provision of information on violation of the law by a Whistleblower through internal or external reporting channels in accordance with the provisions of the Act.
A report may relate to an act or omission that:
• constitutes a violation of the law or internal regulations,
• may lead to a threat to public interest, safety and security or human rights.
Legal basis:
• Articles 25-27 of the Act (internal reports, rules for receipt, confirmation, and protection of confidentiality),
• Article 10-11 of the Act (external reports and the right to choose a channel),
• Articles 7-9 of the Directive (reporting channels),
• Article 54 of the Constitution of the Republic of Poland (right to freedom of expression and provision of information).

2.3 Breach Investigation Team (Team)

The Breach Investigation Team is a body established within the organisation to:
- receive and verify reports of violations of the law,
- carry out an investigation into reports,
- ensure the protection of Whistleblowers from retaliation.

The Team is composed of persons responsible for compliance with regulations on Whistleblower protection and operates according to the principles of confidentiality and impartiality.
The Team consists of the following persons from Stalexport Autostrady and VIA4 S.A.:
- Compliance Officer,
- Deputy Chief Accountant, Proxy (from VIA4 S.A.),
- Toll Manager (from VIA4 S.A.),
- Director of Internal Audit.

Legal basis:
- Article 25(1) of the Act (obligation to establish a body responsible for receiving and examining reports),
- Article 9(1)(a) of the Directive (impartiality and independence of the responsible unit),
- Article 16 of the Directive (principle of confidentiality).

2.4 Team Coordinator (Coordinator)

The Team is coordinated by Compliance Officer who:
- manages the whistleblowing process from receipt of the report to the closure of the investigation,
- has the right to represent the Team.

Legal basis:
- Article 25(1) of the Act (person designated to coordinate the reporting procedure),
- Article 9(1)(b) of the Directive (obligation to ensure proper management of reporting channels),

2.5 Impartiality, conflict of interest and substitutions

- A member of the Breach Investigation Team who may be affected by a report or who is in a conflict of interest (in particular an employment, personal or financial relationship) is required to immediately disclose the conflict and recuse themselves from participation in the matter.

- The Coordinator shall appoint a substitute for the recused member; in the event of a conflict on the part of the Coordinator, the substitute shall be appointed by the Chairman of the Supervisory Board or any other competent body indicated in internal regulations.

- If the report concerns a member of the Management Board, the Supervisory Board or the Director of Internal Audit, the Coordinator shall inform the Chairman of the Supervisory Board and, where necessary, the relevant committees, ensuring an independent investigation procedure.

3. Reporting channels

3.1 Internal reports

Reports may be submitted:
• in electronic form at: **sygnalista@via4.pl**
• by regular mail to the following address: Compliance Officer at VIA 4 S.A., ul. Piaskowa 20, 41-404 Mysłowice
Legal basis:
• Articles 25-27 of the Act (obligation to establish internal channels for receiving reports, confirmation of receipt of report,
• Article 9 of the Directive (procedures for receiving internal reports).

3.2 External reports

In accordance with the provisions of Chapters 4 and 5 of the Act, the Whistleblower has the right to submit an external report to the competent public authority, in particular to:
• the Ombudsman, which accepts reports and provides support in the field of Whistleblower protection,
• other authorities indicated by law, such as supervisory bodies for specific sectors, e.g. the Polish Financial Supervision Authority or the State Labour Inspectorate,
• or to make a public disclosure without prior internal reporting.
Legal basis:
• Articles 30-34 of the Act (external reports),
• Article 10 of the Directive (reports to competent authorities),
• Article 15 of the Act (Whistleblower's right to choose the reporting channel).

4. Processing of reports

4.1 Receipt of reports

Reports are received by members of the Breach Investigation Team.
The Coordinator confirms receipt of the internal report to the Whistleblower within 7 days of its receipt.
Legal basis:
• Article 25(1)(5) of the Act (obligation to confirm receipt within 7 days),
• Article 11(2) of the Directive (confirmation of acceptance of the report).

4.2 Preliminary verification

The completeness and legitimacy of the report shall be verified.
If necessary, the Whistleblower may be asked to provide additional information.
Legal basis:
• Article 25 of the Act (verification of reports and follow-up action),
• Article 12(1) of the Directive (assessment of the report).

4.3. Investigation

The investigation is conducted in a confidential manner.
The Coordinator analyses any incoming reports and:
• if the report contains accurate, detailed, and verifiable information, the Coordinator shall

launch an appropriate investigation;
• otherwise, if the report contains information unsupported by evidence and/or unverifiable information and if the Whistleblower is not available to provide the necessary additional information, the Coordinator shall archive the report;
• if the report relates to any matters that are beyond the scope of this Procedure (e.g. commercial complaints, commercial offers, marketing activities), the Coordinator shall forward the report to the department of VIA 4 S.A. responsible for examining the matter; that department will be responsible for informing the Team of the results of its verification activities within 60 days from the date of acknowledgement of receipt of the internal report.
The maximum time limit for providing feedback to the Whistleblower is 3 months from the date of acknowledgement of receipt of the report.
The feedback includes a description of follow-up action taken or planned and the reason(s) for taking or refraining from taking such action.
Legal basis:
• Article 25 of the Act (conduct of proceedings, confidentiality),
• Article 12(3) of the Directive (3-month deadline for providing feedback).

4.4 Closing of reports

Once the investigation is completed, the report is archived as "substantiated" or "unsubstantiated".
Legal basis:
• Article 25 of the Act (termination of proceedings and documentation),
• Article 13 of the Directive (closure of the report).

5. Protection of Whistleblowers and reported parties

5.1 Prohibition of retaliation

The organisation undertakes to comply with the prohibition of retaliation against Whistleblowers, including:
• dismissal from employment, salary reductions,
• changes in working conditions to the detriment of the Whistleblower,
• harassment, discrimination or other forms of unfavourable treatment.
Legal basis:
• Articles 11-22 of the Act (prohibition of retaliation),
• Article 19 of the Directive.

5.2 Legal remedies

Whistleblowers are protected against legal liability for making a report in good faith.
Whistleblowers may make use of legal assistance and support from public authorities.
Legal basis:
• Articles 11-22 of the Act (Whistleblower's protection against liability),
• Articles 11-22 of the Act (support measures for Whistleblowers),
• Article 16 of the Directive (protection of confidentiality).

5.3 Protection of reported parties

Persons against whom violations have been reported are guaranteed the protection of their reputation and dignity and vested with the right to provide explanations.
Legal basis:
- Articles 11-22 of the Act (protection of the rights of reported parties),
- Article 22 of the Directive (right of defence, protection of reputation).

6. Register of reports

The Coordinator shall keep a record of internal reports;
The Company shall be the controller of any personal data collected in the register of internal reports.
The register of internal reports includes:

1. report number;
2. description of how the law was violated;
3. personal data of the Whistleblower and of the reported party, necessary for identifying these persons;
4. contact address of the Whistleblower;
5. date of submission of the report;
6. information on the follow-up action taken;
7. date of closure of the case.

Personal data and other information in the register of internal reports shall be kept for a period of 3 years after the end of the calendar year in which the follow-up action was completed or after the completion of proceedings initiated by this action.
The files (electronic and hard copies) are stored in a manner ensuring full confidentiality and security, with access restricted to authorised persons.
Legal basis:
- Article 29 of the Act (obligation to maintain a register),
- Article 5(1)(e) of the GDPR (data retention limitation),
- Article 6(1)(c) and (f) of the GDPR (legal grounds for processing).

7. Training and awareness-raising

The Company provides regular training for employees on the reporting procedure and the protection of Whistleblowers. Such training includes:
- reporting methods,
- rules of confidentiality,
- rights vested in and protection measures available to Whistleblowers.

Legal basis:
- Article 25 of the Act (obligation to provide employees with information on the procedure),
- Article 9(1)(b) of the Directive (obligation to provide clear and accessible information),
- Article 94(1) of the Labour Code (employer's obligation to train employees).

8. Sanctions

In accordance with Articles 54-59 of the Whistleblower Protection Act, the Company applies liability and sanctions for breaches of the whistleblowing procedure and the protection of Whistleblowers:

Retaliation
Those who retaliate against Whistleblowers are subject to disciplinary and criminal liability. Pursuant to Article 54 of the Act, retaliation may result in a fine, restriction of liberty, or imprisonment for up to 3 years.

Disclosure of the Whistleblower's identity
Unauthorised disclosure of a Whistleblower's identity without his or her consent is punishable under Article 56 of the Act. This can result in a fine, restriction of liberty, or imprisonment for up to 2 years.

False reports
Submitting a report in bad faith, containing knowingly false information, constitutes a breach of Article 57 of the Act and is punishable by a fine, restriction of liberty, or imprisonment for up to one year.

Failure by the organisation to fulfil its obligations
An organisation that fails to implement an internal reporting system or fails to provide protection to Whistleblowers may be subject to administrative sanctions under Article 58 of the Act.

Obligation to repair damage
If a Whistleblower suffers damage as a result of retaliation, the organisation or person responsible is obligated to compensate for the damage (Article 14 of the Act).

Rules of conduct in the event of a violation
In the event of a violation of the provisions of the Act, the organisation shall take appropriate corrective action to eliminate the effects of the violation and prevent its recurrence.
Legal basis:
- Articles 54-59 of the Act (criminal, civil, and administrative liability),
- Article 23 of the Directive (sanctions for obstructing reports and retaliation).

9. Protection of the personal data of the Whistleblower, the reported party, and any third party indicated in the report

Processing of personal data
(a) VIA4 S.A. shall be the controller of the personal data of the Whistleblower, the reported party and the third party indicated in the report. The Controller has appointed a Data Protection Officer who can be contacted by e-mail at: sygnalista@via4.pl

(b) The personal data of the Whistleblower, the reported party, and any third party indicated in the report shall be processed in accordance with the GDPR and the Act.

(b) Information on the processing of the Whistleblower's personal data is provided in the information clause attached as Appendix 1 to this Procedure.

(c) Information on the processing of personal data of the reported party and any third party indicated in the report is provided in the information clause attached as Appendix 2 to this Procedure.

Legal basis:
- Article 6(1)(c) and 6(1)(f), and Article 9(2)(g) in conjunction with Article 9(1) of the GDPR (legal grounds for processing),
- Article 5(1)(c) and 5(1)(e) of the GDPR (minimisation and limitation of storage),
- Articles 13-15 of the GDPR (information obligation and rights of data subjects),
- Article 29 of the Act (register of reports and data retention period).

---

10. Final provisions

This Procedure shall enter into force on 10 December 2025 based on the resolution of the Management Board of VIA4 S.A. No. 01/12/2025

Appendices:

1. Information clause – Whistleblower

2. Authorisation for data processing – Whistleblower

3. Information clause for the reported party or other person

Notice on the processing of personal data of the Whistleblower

Contact details of the Data Controller:
VIA 4 S.A., with its registered office in Mysłowice
41-404 Mysłowice, ul. Piaskowa 20

Contact details of the Data Protection Officer (DPO):
41-404 Mysłowice, ul. Piaskowa 20
e-mail: iod@via4.pl
phone: +48 32 76 27 512

Purpose and legal basis for processing personal data

Your personal data will be processed for purposes connected with the implementation of the Whistleblowing and Whistleblower Protection Procedure in force at VIA 4 S.A.
The legal basis for processing your personal data are as follows:
- a legal obligation under the Whistleblower Protection Act of 14 June 2024, that is processing whistleblower reports and performing other obligations indicated in the aforementioned Act (i.e. under Article 6(1)(c) of the GDPR);
- the legitimate interest of the Data Controller, that is the archiving of data and documents to demonstrate proper fulfilment of legal obligations, including the establishment, exercise and defence of claims, internal reporting (Article 6(1)(f) of the GDPR);
- your voluntary consent, if you provide consent to the disclosure of your personal data that would allow your identity as the Whistleblower to be established (Article 6(1)(a) of the GDPR).

If the scope of personal data processed in connection with whistleblowing extends to special category data, the legal basis for its processing shall be Article 9(2)(g) of the GDPR in conjunction with Article 9(1) of the GDPR.

Data retention period
Personal data and other information included in the register of internal reports shall be kept for a period of 3 years after the end of the calendar year in which the follow-up action was completed or after the completion of proceedings initiated by this action.
Personal data processed in connection with the receipt of a report or the taking of follow-up action and any documents related to such report shall be retained for a period of 3 years after the end of the calendar year in which the external report was submitted to the public authority competent to undertake follow-up action or in which such follow-up action was completed, or after the completion of proceedings initiated by such action. An exception applies where documents related to the report are part of the files in pre-trial proceedings or court or administrative court cases.
Personal data that are irrelevant to the report under consideration shall not be collected, and if collected accidentally, they shall be deleted immediately (no later than 14 days after it is established that they are not relevant to the matter at hand).

Transfer of data outside the EU/EEA and profiling: Personal data shall not be transferred outside the EU/EEA and shall not be subject to automated decision-making, including profiling.

Provision of personal data:
Provision of personal data is voluntary and does not affect the whistleblowing process, but may affect the execution of this process, for example where additional information is required to handle a report. The consequence of not providing personal data (e.g. a contact address) may also be that no feedback can be provided.

Data recipients:
Data recipients may include entities authorised by law (public authorities) and entities that support the Controller in the fulfilment of the aforementioned purposes of processing under an agreement concluded with such entity, such as law firms, postal service providers, or providers of IT systems used for data processing in connection with the handling of reports. The identity of the Whistleblower may be disclosed to certain entities, e.g. the persons to which the report relates, only if the Whistleblower gives consent.

Rights of data subjects
Depending on the legal bases for the processing of personal data and the conditions referred to in Articles 7 and 15-22 of the GDPR, each data subject has the right to:

a) access his or her personal data and receive copies thereof (Article 15 of the GDPR;
b) request the rectification of data which are incorrect and have incomplete data completed (Article 16 of the GDPR);
c) request the erasure of personal data (Article 17 of the GDPR);
d) request the restriction of personal data processing in the cases specified in Article 18 of the GDPR;
e) data portability in the cases specified in Article 20 of the GDPR;
f) object – on grounds relating to his or her particular situation – at any time to the processing of personal data concerning him or her which is based on Article 6(1)(f) of the GDPR and in other cases referred to in Article 21 of the GDPR;
g) withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal (Article 7 of the GDPR).

In order to exercise any of the aforementioned rights or resolve any doubts related to the assertion of these rights, please submit a request or inquiry to VIA 4 S.A. in the manner provided for in the Whistleblowing and Whistleblower Protection Procedure adopted by the Controller.

h) Data subjects also have the right to lodge a complaint with a supervisory authority if he or she considers that VIA 4 S.A. processes his or her personal data in violation of the applicable law. In Poland, the supervisory authority is the President of the Personal Data Protection Office.

Mysłowice, ...

AUTHORISATION
TO PROCESS PERSONAL DATA

Pursuant to Article 29 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, p. 1) – hereinafter GDPR, in conjunction with Article 27(2) of the Personal Data Protection Act of 14 June 2024 – I hereby authorise:

_____
(full name)

to process ordinary personal data and special categories of personal data of the whistleblower, reported parties, and any third parties identified in the report, collected in connection with the receipt and verification of internal reports, the undertaking of follow-up action, as well as the performance of other legal obligations under the Whistleblower Protection Act of 14 June 2024.

I also oblige you to maintain the confidentiality of all information and personal data obtained in connection with the receipt and verification of internal reports and the undertaking of follow-up actions, both during the term and after the termination of the employment relationship or any other legal relationship under you performed such work.

Validity period of the authorisation: from the moment of signing until revoked.

.....

I hereby confirm that I have read the content of this Authorisation and undertake to maintain the confidentiality of the information and personal data referred to in the Authorisation, including after the termination of the employment relationship or any other legal relationship under which I perform this work.

.....
signature of the authorised person

Date of expiry:
The authorisation was revoked on .....

.....
signature of the person authorised to revoke the authorisation

Notice on the processing of personal data of the person covered by whistleblower report or another person involved in the investigation

Contact details of the Data Controller:
VIA4 S.A., with its registered office in Mysłowice
41-404 Mysłowice, ul. Piaskowa 20

Contact details of the Data Protection Officer (DPO):
41-404 Mysłowice, ul. Piaskowa 20
e-mail: iod@via4.pl
phone: +48 32 76 27 512

Purpose and legal basis for processing personal data

Your personal data will be processed for purposes connected with the implementation of the Whistleblowing and Whistleblower Protection Procedure in force at VIA4 S.A.
The legal basis for processing your personal data are as follows:
- a legal obligation under the Whistleblower Protection Act of 14 June 2024, that is processing whistleblower reports and performing other obligations indicated in the aforementioned Act (i.e. under Article 6(1)(c) of the GDPR);
- the legitimate interest of the Data Controller, that is the archiving of data and documents to demonstrate proper fulfilment of legal obligations, including the establishment, exercise and defence of claims, internal reporting (Article 6(1)(f) of the GDPR);

If the scope of personal data processed in connection with whistleblowing extends to special category data, the legal basis for its processing shall be Article 9(2)(g) of the GDPR in conjunction with Article 9(1) of the GDPR.

Source of personal data:
We received your personal data from a whistleblower or another person involved in an investigation carried out in accordance with the Whistleblowing and Whistleblower Protection Procedure.

Scope of personal data processed:
We process basic identification data indicated in the whistleblower report and information obtained during an ongoing investigation. This information may include special categories of personal data referred to in Article 9(1) of the GDPR (if included in the whistleblower report or obtained during an ongoing investigation).

Data retention period
Personal data will be stored no longer than necessary for the above purposes.
In view of the above, personal data processed in connection with the receipt of a report or the taking of follow-up action and any documents related to such report shall be retained for a period of 3 years after the end of the calendar year in which the external report was submitted to the public authority competent to undertake follow-up action or in which such follow-up action was completed, or after the completion of proceedings initiated by such action. An exception applies where documents related to the report are part of the files in pre-trial proceedings or court or administrative court cases.
Personal data that are irrelevant to the report under consideration shall not be collected, and if collected accidentally, they shall be deleted immediately (no later than 14 days after it is established that they are not relevant to the matter at hand).

Transfer of data outside the EU/EEA and profiling: Personal data shall not be transferred outside the EU/EEA and shall not be subject to automated decision-making, including profiling.

Data recipients:
Data recipients may include entities authorised by law (public authorities) and entities that support the Controller in the fulfilment of the aforementioned purposes of processing under an agreement concluded with such entity, such as law firms, postal service providers, or providers of IT systems used for data processing in connection with the handling of reports.

Rights of data subjects
Depending on the legal bases for the processing of personal data and the conditions referred to in Articles 7 and 15-22 of the GDPR, each data subject has the right to:

a) access his or her personal data and receive copies thereof (Article 15 of the GDPR;
b) request the rectification of data which are incorrect and have incomplete data completed (Article 16 of the GDPR);
c) request the erasure of personal data (Article 17 of the GDPR);
d) request the restriction of personal data processing in the cases specified in Article 18 of the GDPR;
e) object – on grounds relating to his or her particular situation – at any time to the processing of personal data concerning him or her which is based on Article 6(1)(f) of the GDPR and in other cases referred to in Article 21 of the GDPR;

In order to exercise any of the aforementioned rights or resolve any doubts related to the assertion of these rights, please submit a request or inquiry to VIA4 S.A. in the manner provided for in the Whistleblowing and Whistleblower Protection Procedure adopted by the Controller.

f) Data subjects also have the right to lodge a complaint with a supervisory authority if he or she considers that VIA4 S.A. processes his or her personal data in violation of the applicable law. In Poland, the supervisory authority is the President of the Personal Data Protection Office.