

# Whistleblowing and Whistleblower Protection Procedure

## Table of Contents

1.	General Provisions .....	2
2.	Definitions .....	3
3.	Reporting Channels.....	4
4.	Confidentiality and Personal Data Protection .....	6
5.	Protection Against Retaliation .....	8
6.	Information Required in a Report.....	8
7.	Management of Reports.....	9
8.	Procedure for Reports Concerning Members of the GPW Management Board or the GPW Supervisory Board .....	12
9.	External Reporting .....	13
10.	Appendices .....	15

## **1. General Provisions**

---

### **1.1**

GPW is committed to maintaining high ethical standards and expects its employees to act in accordance with these values, including reporting any reasonable suspicions of Breaches with due diligence. GPW ensures the confidentiality of information reported in relation to Breaches.

### **1.2**

This Procedure implements the obligations set out in:

- Article 24 of the Polish Act on the Protection of Whistleblowers;
- Article 32(3) of the Market Abuse Regulation;
- Article 25e(1) of the Act on Trading in Financial Instruments;
- Article 97d of the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies;
- Article 53 of the Anti-Money Laundering and Counter-Terrorist Financing Act;
- Article 6(1) of the Corporate Governance Principles for Supervised Institutions of 22 July 2014; and
- the Recommended Standards for Compliance Management Systems in the Area of Anti-Corruption and Whistleblower Protection in Companies Listed on Markets Operated by Giełda Papierów Wartościowych w Warszawie S.A.

### **1.3**

This Procedure applies directly to reports submitted under the Anti-Corruption and Fraud Prevention Policy at GPW. In matters covered by the Anti-Mobbing Policy of Giełda Papierów Wartościowych w Warszawie S.A., the dedicated reporting procedure specified in that policy shall apply.

### **1.4**

This document specifies:

- a. events subject to reporting under this Procedure ("Breaches")<sup>1</sup>;
- b. reporting channels, including dedicated communication channels;
- c. confidentiality principles applicable to the investigation of reported information;
- d. information required for the assessment of a Report;
- e. principles governing the protection of personal data of the Reporting Person, the Person Concerned, and any other person identified in a Report;
- f. measures protecting the Whistleblower, including protection against retaliation, discrimination, or other forms of unfair treatment;
- g. the process for handling and managing Reports, including:
  - the nature of Follow-up Actions undertaken after receipt of a Report;
  - the retention and deletion periods applicable to personal data contained in Reports.

### **1.5**

Employees acknowledge that they have read and accepted this Procedure by signing the declaration attached as Appendix 1.

### **1.6**

DCO is responsible for providing initial and periodic training to employees regarding the reporting of Breaches.

### **1.7**

DCO shall review this Procedure at least annually and update it whenever necessary.

---

<sup>1</sup> excluding conflicts of interest, which are handled in accordance with the principles set out in the Rules for Managing Conflicts of Interest at GPW.

## 2. Definitions

---

For the purposes of this Procedure:

**AMLU** – the Act of 1 March 2018 on Anti-Money Laundering and Counter-Terrorist Financing.

**CO (Compliance Officer)** – a function performed by:

- a person employed as Director or Deputy Director of DCO; or
- another person designated by the Management Board Member responsible for DCO, provided that such person holds a position no lower than Expert within DCO.

**DCO** – Compliance Department.

**DWW** – Internal Audit Department.

**Retaliation** – any direct or indirect act or omission occurring in a work-related context that is caused by a Report or Public Disclosure and that causes or may cause unjustified harm to a Whistleblower or infringes or may infringe the Whistleblower's rights.

Retaliation includes in particular:

- reduction of remuneration;
- limitation of promotion or career development opportunities;
- ostracism;
- workplace bullying;
- discriminatory treatment;
- unfair treatment;
- actions adversely affecting the legal or factual situation of the Whistleblower;
- threats;
- disciplinary measures, reprimands, or other sanctions, including financial penalties.

**Follow-up Action** – any action taken by a legal entity or public authority to assess the accuracy of information contained in a Report and to address the reported Breach, including investigations, inspections, administrative proceedings, prosecution, recovery of funds, or closure of proceedings under an internal or external reporting procedure.

**GPW** – Giełda Papierów Wartościowych w Warszawie S.A. (Warsaw Stock Exchange S.A.).

**Breach** – an actual or potential violation (i.e. a violation for which there is a real risk of occurrence), or a reasonable suspicion of a violation, of internal regulations, applicable laws, or adopted standards, that has occurred or may occur within GPW.

**Person Concerned** – a natural person, legal entity, or organizational unit with legal capacity identified in a Report or Public Disclosure as the person who committed a Breach or as a person associated with such individual.

**Facilitator** – a natural person who assists a Whistleblower in making a Report or Public Disclosure in a work-related context and whose identity and involvement must remain confidential.

**Person Associated with a Whistleblower** – a natural person who may experience Retaliation, including a colleague or a close relative within the meaning of Article 115 §11 of the Polish Criminal Code.

**Whistleblower** – any natural person who reports information concerning a Breach obtained in a work-related context, including:

- employees;
- contractors;
- service providers;
- entrepreneurs;
- commercial proxies;
- GPW shareholders;

- members of the GPW Management Board;
- members of the GPW Supervisory Board;
- persons working under the supervision of contractors, subcontractors, or suppliers;
- interns, trainees, and volunteers;
- candidates applying for cooperation with GPW.

Whistleblower status also applies to persons reporting information obtained before the commencement of a work relationship or after its termination.

**Procedure** – this Whistleblowing and Whistleblower Protection Procedure.

**Breaches Register** – the electronic register of Reports, including anonymous Reports, maintained by DCO in accordance with Appendix 2.

**GPW Supervisory Board (GSB)** – the Supervisory Board of Giełda Papierów Wartościowych w Warszawie S.A.

**Market Abuse Regulation (MAR)** – Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse.

**Whistleblower Protection Act** – the Act of 14 June 2024 on the Protection of Whistleblowers.

**GPW Management Board (GMB)** – the Management Board of Giełda Papierów Wartościowych w Warszawie S.A.

**Report** – information concerning observed Breaches submitted by a Whistleblower in accordance with this Procedure.

### **3. Reporting Channels**

---

#### **3.1**

The following categories of legal violations may be reported under the Whistleblower Protection Act:

- a. corruption;
- b. public procurement;
- c. financial services, products and markets;
- d. anti-money laundering and counter-terrorist financing;
- e. product safety and compliance;
- f. transport safety;
- g. environmental protection;
- h. radiation protection and nuclear safety;
- i. food and feed safety;
- j. animal health and welfare;
- k. public health;
- l. consumer protection;
- m. privacy and personal data protection;
- n. security of network and information systems;
- o. financial interests of the Republic of Poland, local government units, and the European Union;
- p. the internal market of the European Union, including competition law, state aid rules, and corporate taxation;
- q. constitutional rights and freedoms of individuals and citizens in their relations with public authorities.

#### **3.2**

The following may also be reported under this Procedure:

- a. breaches of employee obligations, subject to Section 1.3;

- b. breaches of the Code of Ethics;
- c. suspected misuse of inside information or professional secrecy, unlawful disclosure of such information, or market manipulation involving financial instruments;
- d. corruption and fraud-related matters covered by the Anti-Corruption and Fraud Prevention Policy at GPW.

### 3.3

The categories referred to in Section 3.2 constitute an extension of the statutory whistleblowing framework to include violations of internal regulations and ethical standards.

Reports concerning such matters may only be submitted through GPW's internal reporting channels and may not form the basis for external reporting under the Whistleblower Protection Act.

### 3.4

Where a Report concerns:

- personal data breaches,
- information security incidents,
- operational incidents,
- anti-money laundering or counter-terrorist financing obligations,

the CO or an authorized DCO employee shall provide the information, to the extent necessary, to the relevant function holder (Data Protection Officer, Security Officer, Risk Officer, or AML Officer), in accordance with the need-to-know principle.

### 3.5

Personal data of Whistleblowers and Persons Concerned shall not be processed for purposes other than those arising directly from this Procedure and applicable law.

### 3.6

A Whistleblower may submit a Report through:

- the dedicated email address: **naruszenia@gpw.pl**;
- the GPW Registry Office;
- traditional mail;
- telephone contact with the CO or an authorized DCO employee;
- written correspondence addressed to CO/DCO marked "**Private and Confidential**".

### 3.7

Where the Breach concerns actions or omissions of DCO or the CO, the Whistleblower may submit a Report in person through the GPW Registry Office, by traditional mail addressed to the President or Vice-President of the GPW Management Board and marked "Private and Confidential", or by email sent directly to the President or Vice-President of the GPW Management Board.

### 3.8

A Whistleblower may also submit a Report pursuant to Article 25e(1) of the Act on Trading in Financial Instruments or Article 97d of the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies directly to:

- a. the GPW Supervisory Board at: **RN.naruszenia@gpw.pl**;
- b. the President of the GPW Management Board via his or her business email address.

### 3.9

Where a Report is submitted by telephone or in person, a written record of the conversation shall be prepared and made available to the Whistleblower for verification of its contents.

The Whistleblower shall have the opportunity to review, correct, and confirm the information contained in the record, either in writing or electronically by email, and to sign the record.

A template of the record is attached as Appendix 3.

### **3.10**

A Report may also be submitted in writing and sent to the registered office of GPW addressed to one of the persons referred to above and marked "Private and Confidential." Reports may be submitted anonymously.

### **3.11**

Anonymous Reports may be submitted, for example, through an anonymous email address or by submitting a printed document without identifying information. Sections 3.6–3.10 shall apply accordingly. GPW will not undertake any actions aimed at identifying the person who submitted an anonymous Report. No feedback shall be provided to persons submitting anonymous Reports.

### **3.12**

The CO, an authorized DCO employee, or another authorized person receiving a Report shall acknowledge receipt of the Report within seven days of its receipt, unless the Whistleblower has not provided contact details.

## **4. Confidentiality and Personal Data Protection**

---

### **4.1**

As the controller of personal data, GPW exercises particular care in protecting the interests of the Whistleblower, the Person Concerned, and any individuals identified in a Report.

GPW applies appropriate technical and organizational measures to ensure the protection of personal data against unauthorized access, in accordance with Regulation (EU) 2016/679 (GDPR).

GPW ensures that personal data shall be:

#### **4.1.1**

Processed lawfully, fairly, and transparently. (*Principle of lawfulness, fairness, and transparency – Article 5(1)(a) GDPR*).

#### **4.1.2**

Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. (*Purpose limitation principle – Article 5(1)(b) GDPR*).

#### **4.1.3**

Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. (*Data minimisation principle – Article 5(1)(c) GDPR*).

#### **4.1.4**

Accurate and, where necessary, kept up to date. (*Accuracy principle – Article 5(1)(d) GDPR*).

#### **4.1.5**

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed. (*Storage limitation principle – Article 5(1)(e) GDPR*).

#### **4.1.6**

Processed in a manner ensuring appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. (*Integrity and confidentiality principle – Article 5(1)(f) GDPR*).

### **4.2**

Pursuant to Article 14 GDPR, GPW informs Persons Concerned and other individuals identified in a Report about the processing of their personal data, excluding information concerning the source of the personal data, unless:

- the Whistleblower does not meet the conditions specified in Article 6 of the Whistleblower Protection Act; or
- the Whistleblower has expressly consented to disclosure of their identity.

#### **4.3**

Information notices concerning the processing of personal data of:

- the Whistleblower,
- the Person Concerned, and
- persons identified in a Report,

are attached as Appendices 4, 5, and 6 to this Procedure, respectively.

#### **4.4**

GPW fulfils requests for access to personal data submitted by Persons Concerned and persons identified in a Report, excluding information regarding the source of the personal data, unless:

- the Whistleblower does not meet the conditions specified in Article 6 of the Whistleblower Protection Act; or
- the Whistleblower has expressly consented to disclosure of their identity.

#### **4.5**

Personal data and other information contained in the Breaches Register, as well as personal data processed in connection with Reports, Follow-up Actions, and related documentation, shall be retained:

a. For Reports submitted under the Whistleblower Protection Act:

for a period of three years after the end of the calendar year in which Follow-up Actions were completed or proceedings initiated by such actions were concluded.

b. For Reports submitted under:

- the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies;
- the Market Abuse Regulation;
- the Act on Trading in Financial Instruments;
- the Anti-Money Laundering and Counter-Terrorist Financing Act;

for a period of five years, calculated from the first day of the year following the year in which the documents or information carriers were created or received.

Where a Report concerns internal regulations, procedures, or other internal rules, the five-year retention period shall be calculated from the first day of the year following the year in which such regulations ceased to apply.

#### **4.6**

Upon expiry of the applicable retention period, GPW shall delete personal data and destroy documents related to the Report.

#### **4.7**

Section 4.6 shall not apply where the documents related to a Report form part of criminal investigations, court proceedings, or administrative court proceedings.

#### **4.8**

Personal data shall be processed for the purposes of maintaining the Breaches Register and handling reported Breaches in accordance with the GDPR. Access to the Breaches Register is restricted exclusively to authorized DCO employees.

#### **4.9**

Processing is necessary for compliance with a legal obligation to which GPW is subject pursuant to Article 6(1)(c) GDPR.

The legal basis for processing includes, in particular:

- Article 32(3) of the Market Abuse Regulation;
- Article 25e(1) of the Act on Trading in Financial Instruments;

- Article 97d of the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies;
- Article 53 of the Anti-Money Laundering and Counter-Terrorist Financing Act;
- Article 24(1) of the Whistleblower Protection Act.

#### **4.10**

GPW ensures the confidentiality of:

- Reports;
- information obtained during investigations;
- information stored in the Breaches Register; and
- personal data of Whistleblowers and individuals identified in Reports.

The identity of a Whistleblower shall not be disclosed except in circumstances provided for by this Procedure or by applicable law.

#### **4.11**

Whistleblowers are required to provide truthful information and to submit Reports in a manner that does not violate the personal dignity of any individual.

#### **4.12**

Persons responsible for receiving, handling, verifying, and investigating Reports may perform such activities only after receiving a written authorization granted by the GPW Management Board.

Such persons are required to maintain confidentiality regarding all information and personal data obtained in connection with Reports and Follow-up Actions, including after termination of their employment or other legal relationship with GPW.

## **5. Protection Against Retaliation**

---

### **5.1**

GPW shall not undertake any Retaliatory Actions against Whistleblowers, Facilitators, Persons Associated with a Whistleblower, legal entities, or organizational units assisting or associated with a Whistleblower, including, in particular, entities owned by or employing the Whistleblower.

### **5.2**

A Whistleblower who experiences any form of Retaliatory Action should immediately inform the CO, an authorized DCO employee, or the GPW Management Board. Where the Report concerns an act or omission of the CO or DCO, the Whistleblower should notify the Director of the Internal Audit Department authorized to handle such matters. Such reports shall be subject to a separate investigation conducted in a manner ensuring the broadest possible protection of the Whistleblower.

### **5.3**

Section 5.1 shall apply accordingly to employees and other persons acting on behalf of GPW who perform duties related to the obligations referred to in Articles 74, 86, 89, and 90 of the Anti-Money Laundering and Counter-Terrorist Financing Act (AMLU).

### **5.4**

A Whistleblower shall not be entitled to the protection provided under this Procedure if they did not have reasonable grounds to believe that the information reported was true and that it concerned a Breach.

## **6. Information Required in a Report**

---

### **6.1**

Only events that can be identified and verified for the purpose of conducting an investigation may be reported under this Procedure.

## **6.2**

If the information provided by the Whistleblower is insufficient to identify the Breach and it is not possible to obtain additional information, the Report shall not be processed.

## **6.3**

A Report should include, in particular:

- a. identifying information enabling contact with the Whistleblower, except in the case of anonymous Reports referred to in Section 3.11;
- b. the name of the organizational unit or the details of the person concerned by the Report;
- c. information regarding other persons who may be connected with the matters described in the Report;
- d. a concise description of the matter, including all information available to the Whistleblower concerning the Breach.

## **7. Management of Reports**

---

*(excluding Reports concerning members of the GPW Management Board or the GPW Supervisory Board)*

### **7.1**

Activities related to receiving and verifying internal reports of legal breaches, undertaking Follow-up Actions, and processing personal data in connection with such reports may only be carried out by persons holding a specific written authorization granted by the GPW Management Board.

The template authorization is attached as Appendix 7 to this Procedure.

In the case of the Director of DCO, the authorization shall additionally specify that the GPW Management Board authorizes the Director of DCO to grant further individual authorizations solely in relation to a specific internal Report, as referred to in Section 7.2.

### **7.2**

The Director of DCO, or in the Director's absence the GPW Management Board, may grant a specific written authorization relating exclusively to a particular internal Report.

Such authorization shall cover activities relating to:

- receiving and verifying the Report;
- undertaking Follow-up Actions;
- processing personal data necessary for handling the Report.

Authorizations may only be granted to persons whose involvement is necessary for handling the specific Report. The authorization template is attached as Appendix 8.

### **7.3**

Access to information concerning a Report and Follow-up Actions shall be restricted in accordance with the need-to-know principle as defined in the GPW Information Security Policy.

Access shall be limited to persons participating in the handling of the Report and holding written authorizations referred to in Sections 7.1 and 7.2.

The scope of information shared shall be limited to data necessary for the performance of a given role. In particular, persons providing explanations shall not have access to all information available to those investigating the Report, but only to information necessary to enable them to provide complete explanations.

### **7.4**

Only Reports for which a decision has been made to initiate proceedings shall be entered into the Breaches Register maintained in accordance with Appendix 2. Registration shall be performed by the CO or an authorized DCO employee or another authorized GPW representative (in the case of Reports

concerning the CO/DCO, members of the GPW Supervisory Board, or members of the GPW Management Board).

#### **7.5**

Where a Report is received by the GPW Management Board or the GPW Supervisory Board, information concerning the Report shall be forwarded to the CO or an authorized DCO employee for preliminary assessment and, where appropriate, investigation. Where a decision is made to proceed with an investigation, the CO or authorized DCO employee shall register the Report in the Breaches Register. If the Report concerns actions or omissions of the CO or DCO, the Report shall instead be referred to the Director of the Internal Audit Department or an authorized employee of the Internal Audit Department. For the purposes of handling and assessing such Reports, support from an external service provider may be engaged to ensure impartiality.

#### **7.6**

Where a Report concerns the CO or another DCO employee, the investigation may also be conducted by an independent person authorized by the GPW Management Board.

#### **7.7**

Whistleblower status and the protections provided under this Procedure shall apply from the moment a Report is submitted, provided that the reporting person had reasonable grounds to believe that the information reported was true at the time of reporting and that the Report relates to a work-related context as defined in this Procedure. Reports submitted by persons having no professional or work-related connection with GPW shall not qualify for Whistleblower protection.

#### **7.8**

Reports submitted by persons who have no professional relationship with GPW and are not connected with GPW through any legal or factual work-related relationship may:

- a. be left without further consideration; or
- b. be handled under separate internal regulations, subject to those regulations.

#### **7.9**

Upon receipt of a Report, the CO or an authorized DCO employee shall promptly conduct a preliminary assessment and determine whether an investigation should be initiated. Investigations shall be conducted by the CO or DCO and shall aim to establish the facts of the matter.

#### **7.10**

Where a Report lacks sufficient information for verification, the CO or DCO shall, where possible, contact the Whistleblower and request additional information within a specified deadline.

#### **7.11**

If the requested information is not provided within the prescribed deadline, DCO may decide not to proceed with an investigation due to insufficient information.

#### **7.12**

DCO may also decide not to proceed where, despite obtaining additional information or reviewing available data, it is not possible to clearly determine the nature of the alleged Breach or conduct an investigation in a reliable and effective manner.

#### **7.13**

At any stage of the proceedings, the CO, an authorized DCO employee, another organizational unit, or an external auditor may request additional information from the Whistleblower concerning the Report.

#### **7.14**

The CO, an authorized DCO employee, another authorized organizational unit, or an external auditor may request information or documents from GPW employees relating to the Report.

Such information or documents shall be provided without undue delay and no later than within five business days.

#### **7.15**

Where expert knowledge is required, the CO, an authorized DCO employee, another authorized organizational unit, or an external auditor may establish an advisory committee composed of employees from other departments.

Members of the committee shall participate in the proceedings in an advisory capacity.

The composition of the committee shall be determined based on the subject matter of the Report.

The CO or authorized DCO employee shall request that the GPW Management Board grant committee members written authorization to process personal data related to the investigation.

The authorization template is attached as Appendix 8.

#### **7.16**

The Person Concerned shall have the right to review the case file and provide explanations during the investigation, subject to the anonymization of personal data and any information that could identify the Whistleblower.

#### **7.17**

Following completion of the investigation, the CO, authorized DCO employee, authorized organizational unit, or external auditor shall prepare findings and recommendations concerning further actions and the management of the reported Breach.

Where specialist expertise is required, the CO or another authorized person conducting the investigation may request that the GPW Management Board appoint an external expert.

#### **7.18**

The results of the investigation and related recommendations shall be documented in a report prepared by the CO, authorized DCO employee, authorized organizational unit, or external auditor.

The report shall be retained:

- for three years following the end of the calendar year in which Follow-up Actions were completed or proceedings initiated by those actions were concluded, in the case of Reports submitted under the Whistleblower Protection Act; or
- for five years in the case of Reports submitted under the Act on Trading in Financial Instruments, the Act on Public Offering, the Market Abuse Regulation, or the Anti-Money Laundering and Counter-Terrorist Financing Act, in accordance with the retention periods specified in Section 4.5.

#### **7.19**

Persons who are the subject of a Report or who may be affected by a Report shall be excluded from participation in the handling of the matter. Such exclusion shall be documented.

#### **7.20**

Based on the report, supporting documentation, and recommendations received from the CO, another organizational unit, or an external auditor, the GPW Management Board or the GPW Supervisory Board shall decide on the appropriate course of action.

#### **7.21**

The final decision of the GPW Management Board or the GPW Supervisory Board regarding the identified Breach shall be communicated without undue delay to the CO, an authorized DCO employee, another authorized organizational unit, and the Director of the HR Department.

The Director of the HR Department shall inform the employee who was the subject of the investigation of the decision taken by the GPW Management Board.

Such notification shall be made while maintaining the confidentiality of the Whistleblower's identity.

### **7.22**

The decision referred to above shall be recorded in the Breaches Register by the CO, an authorized DCO employee, another authorized organizational unit, or an external auditor.

### **7.23**

Where a Report has been submitted anonymously, an investigation shall be initiated only if:

- the Report contains sufficient information to enable further action; and
- the preliminary assessment confirms its credibility.

### **7.24**

The CO, an authorized DCO employee, or another authorized person responsible for handling the Report shall provide feedback to the Whistleblower within **three months** of acknowledging receipt of the Report, unless the Whistleblower has not provided contact details.

### **7.25**

Once a year, the CO or an authorized DCO employee shall prepare and submit a report summarizing the Reports received during the previous year, including their subject matter and the outcome of the investigations conducted.

The report shall be submitted to the GPW Management Board and the GPW Supervisory Board by the end of the first quarter of each year.

### **7.26**

Confirmed Breaches shall be reported by the CO or an authorized DCO employee to the operational incidents database.

Such reporting shall include only numerical data and statistical information and shall not contain any personal data capable of directly or indirectly identifying a Whistleblower or any other natural person.

### **7.27**

The scope of information reported pursuant to Section 7.26 shall be limited in accordance with:

- the principle of data minimization; and
- the obligation to maintain the confidentiality of the Whistleblower's identity under the Act of 14 June 2024 on the Protection of Whistleblowers,

which prohibits the disclosure of information that could reveal the Whistleblower's identity without the Whistleblower's explicit consent.

## **8. Procedure for Reports Concerning Members of the GPW Management Board or the GPW Supervisory Board**

---

### **8.1**

Where a Report concerns the actions or omissions of a member of the GPW Management Board or the GPW Supervisory Board, the Whistleblower may submit the Report to the Chair of the GPW Supervisory Board or a designated member of the Audit Committee:

- in person through the GPW Registry Office;
- by traditional mail marked "Private and Confidential"; or
- by email to: [RN.naruszenia@gpw.pl](mailto:RN.naruszenia@gpw.pl).

### **8.2**

Where the CO or DCO receives a Report concerning members of the GPW Management Board or the GPW Supervisory Board, information about the Report shall be immediately forwarded to the Chair of the GPW Supervisory Board or a designated member of the Audit Committee.

### **8.3**

Upon receipt of the Report, the Chair of the GPW Supervisory Board, a designated member of the Audit Committee, or another designated GPW employee or external person shall promptly conduct a preliminary assessment of the Report to determine whether an investigation should be initiated.

#### **8.4**

The GPW Supervisory Board or the Audit Committee shall decide whether to initiate an investigation and shall designate the organizational unit or individuals responsible for carrying out the subsequent stages of the proceedings.

The designated unit or individuals shall be responsible for:

- establishing the facts of the matter;
- gathering evidence;
- analyzing the collected material; and
- preparing appropriate conclusions and recommendations.

The designated unit or individuals shall perform their duties in compliance with applicable laws and internal regulations.

The GPW Supervisory Board or the Audit Committee may also define:

- the detailed scope of activities;
- deadlines for completion; and
- reporting requirements.

#### **8.5**

For the purposes of handling and assessing the Report, the GPW Supervisory Board or the Audit Committee may engage an external service provider to support the impartiality of the investigation and assessment of the reported Breach.

#### **8.6**

Registration of a Report concerning a Breach in the Breaches Register shall be carried out in accordance with Section 7.4 of this Procedure.

#### **8.7**

For Reports concerning members of the GPW Supervisory Board or the GPW Management Board, the provisions of Sections 7.5–7.6 and 7.8–7.16 shall apply accordingly, subject to any modifications required by the nature of the Report and the governing body concerned.

#### **8.8**

Based on the report, supporting documentation, and recommendations received from the designated unit or person responsible for conducting the investigation, the GPW Supervisory Board or the Audit Committee shall decide on the appropriate course of action.

#### **8.9**

The decision referred to above shall be recorded in the Breaches Register.

#### **8.10**

Where a Report has been submitted anonymously, an investigation shall be initiated only if:

- the Report contains sufficient information to enable further action; and
- the preliminary assessment confirms its credibility.

#### **8.11**

The organizational unit or individual designated by the GPW Supervisory Board or the Audit Committee shall provide feedback to the Whistleblower within **three months** of acknowledging receipt of the Report, unless the Whistleblower has not provided contact details.

## **9. External Reporting**

---

### **9.1**

A Whistleblower has the right to submit an external report to:

- a. the Commissioner for Human Rights (Ombudsman);

- b. a public authority competent to receive reports concerning Breaches within its area of responsibility;
- c. an institution, body, office, or agency of the European Union.

**9.2**

External reports shall be submitted in accordance with the reporting procedures established by the relevant authority, institution, or body.

Information regarding external reporting channels is available on the websites of:

- the Office of the Commissioner for Human Rights;
- the relevant public authorities; and
- the relevant European Union institutions and bodies.

## 10. Appendices

---

### **Information Notice for Whistleblowers**

#### **Information on the Processing of Personal Data of Whistleblowers by GPW**

This information notice is provided pursuant to Article 13 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, "GDPR").

#### **1. Data Controller**

The controller of personal data is **Giełda Papierów Wartościowych w Warszawie S.A. (GPW)**, ul. Książęca 4, 00-498 Warsaw, Poland, tel. +48 22 628 32 32, email: gpw@gpw.pl.

#### **2. Data Protection Officer**

GPW has appointed a Data Protection Officer, who may be contacted at: **iod@gkgpw.pl**.

#### **3. Purposes and Legal Basis for Processing**

Where a Whistleblower provides personal data, such data will be processed only to the extent necessary for handling reports of Breaches, on the basis of:

##### **1) Article 6(1)(c) GDPR – compliance with a legal obligation**

in connection with:

- a. the Act of 14 June 2024 on the Protection of Whistleblowers; or
- b. the Act of 29 July 2005 on Trading in Financial Instruments; or
- c. the Act of 29 July 2005 on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies; or
- d. the Act of 1 March 2018 on Anti-Money Laundering and Counter-Terrorist Financing; or
- e. Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation – MAR).

##### **2) Article 9(2)(g) GDPR – substantial public interest**

in connection with the above legislation, where special categories of personal data are included in the Whistleblower's Report.

##### **3) Article 9(2)(b) GDPR – employment, social security and social protection obligations and rights**

in connection with the above legislation, where special categories of personal data are included in the Whistleblower's Report.

#### **4. Recipients of Personal Data**

Personal data will be disclosed only to entities authorized to process such data under applicable law, in particular competent public authorities where Follow-up Actions are undertaken in connection with a reported Breach and in accordance with GPW's Whistleblower Protection Procedure.

Personal data may also be entrusted to entities providing services to GPW under contractual arrangements, such as IT service providers.

#### **5. Retention Period**

Personal data will be processed for:

**1)** Three years following the end of the calendar year in which Follow-up Actions were completed or proceedings initiated by those actions were concluded, in the case of Reports submitted under the Whistleblower Protection Act.

**2)** Five years, counted from the first day of the year following the year in which documents or information carriers were created or received, and in the case of internal rules, procedures, and other internal regulations, from the first day of the year following the year in which they ceased to apply, where the Report was submitted under:

- the Act on Trading in Financial Instruments;
- the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies;
- the Market Abuse Regulation;
- the Anti-Money Laundering and Counter-Terrorist Financing Act.

#### **6. Rights of the Data Subject**

You have the right to:

- access your personal data;
- rectify your personal data;
- request erasure of your personal data in cases provided for by law;
- request restriction of processing.

#### **7. Right to Lodge a Complaint**

You have the right to lodge a complaint with the President of the Personal Data Protection Office if you believe that the processing of your personal data violates the GDPR.

## **8. Provision of Personal Data**

The provision of personal data is voluntary.

## **9. Automated Decision-Making**

Personal data will not be subject to profiling and no automated decision-making will be carried out on the basis of such data.

## **Information Notice for the Person Concerned by a Whistleblower Report**

### **Information on the Processing of Personal Data of the Person Concerned by a Whistleblower Report by GPW**

This information notice is provided pursuant to Article 14 GDPR.

#### **1. Data Controller**

The controller of personal data is **Giełda Papierów Wartościowych w Warszawie S.A. (GPW, the Controller)**, ul. Książęca 4, 00-498 Warsaw, Poland, tel. +48 22 628 32 32, email: [gpw@gpw.pl](mailto:gpw@gpw.pl).

#### **2. Data Protection Officer**

The Data Protection Officer may be contacted at: [iodgkgpw@gpw.pl](mailto:iodgkgpw@gpw.pl).

#### **3. Purposes and Legal Basis for Processing**

Personal data will be processed solely to the extent necessary for handling reports of Breaches on the basis of:

##### **1) Article 6(1)(c) GDPR – compliance with a legal obligation**

in connection with:

- a. the Act of 14 June 2024 on the Protection of Whistleblowers ("the Act");
- b. the Act on Trading in Financial Instruments;
- c. the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies;
- d. the Act on Anti-Money Laundering and Counter-Terrorist Financing;
- e. Regulation (EU) No 596/2014 on market abuse (MAR).

##### **2) Article 9(2)(g) GDPR – substantial public interest**

where special categories of personal data are included in the Whistleblower's Report.

#### **4. Categories of Data Processed**

The Controller will process personal data indicated in the Whistleblower's Report concerning the Person Concerned, understood as a natural person identified in the Report or a person associated with an individual who allegedly committed a Breach.

#### **5. Recipients of Personal Data**

Personal data will be disclosed only to entities authorized under applicable law, in particular competent public authorities where Follow-up Actions are undertaken in connection with a reported Breach and in accordance with GPW's Whistleblower Protection Procedure.

Personal data may also be entrusted to service providers acting on behalf of GPW, such as IT service providers.

## **6. Source of Personal Data**

Your personal data were provided by the Whistleblower.

## **7. Retention Period**

Personal data will be processed for:

- 1)** Three years following the end of the calendar year in which Follow-up Actions were completed or proceedings initiated by those actions were concluded, in the case of Reports submitted under the Act.
- 2)** Five years, counted from the first day of the year following the year in which documents or information carriers were created or received and, in the case of internal rules, procedures, and other internal regulations, from the first day of the year following the year in which they ceased to apply, where the Report was submitted under the financial-market or AML regulations referred to above.

## **8. Right of Access**

You have the right to access your personal data, except that Article 15(1)(g) GDPR concerning information about the source of personal data shall not apply unless:

- the Whistleblower does not meet the conditions specified in Article 6 of the Act; or
- the Whistleblower has expressly consented to disclosure of their identity.

## **9. Other Rights**

You have the right to:

- rectify personal data;
- request erasure where permitted by law;
- request restriction of processing.

## **10. Right to Lodge a Complaint**

You have the right to lodge a complaint with the President of the Personal Data Protection Office if you believe that the processing of your personal data violates the GDPR.

## **11. Automated Decision-Making**

## Whistleblowing and Whistleblower Protection Procedure

Personal data will not be subject to profiling and no automated decision-making will be carried out on the basis of such data.

**Information Notice for a Third Party Identified in a Whistleblower Report**

**Information on the Processing of Personal Data of a Third Party Identified in a Whistleblower Report by GPW**

This information notice is provided pursuant to Article 14 GDPR.

**1. Data Controller**

The controller of personal data is **Giełda Papierów Wartościowych w Warszawie S.A. (GPW, the Controller)**, ul. Książęca 4, 00-498 Warsaw, Poland, tel. +48 22 628 32 32, email: [gpw@gpw.pl](mailto:gpw@gpw.pl).

**2. Data Protection Officer**

The Data Protection Officer may be contacted at: [iodgkgpw@gpw.pl](mailto:iodgkgpw@gpw.pl).

**3. Purposes and Legal Basis for Processing**

Personal data will be processed solely to the extent necessary for handling reports of Breaches on the basis of:

**1) Article 6(1)(c) GDPR – compliance with a legal obligation**

in connection with:

- a. the Act of 14 June 2024 on the Protection of Whistleblowers ("the Act");
- b. the Act on Trading in Financial Instruments;
- c. the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies;
- d. the Act on Anti-Money Laundering and Counter-Terrorist Financing;
- e. Regulation (EU) No 596/2014 on market abuse (MAR).

**2) Article 9(2)(g) GDPR – substantial public interest**

where special categories of personal data are included in the Whistleblower's Report.

**4. Categories of Data Processed**

The Controller will process personal data identified in the Whistleblower's Report.

**5. Recipients of Personal Data**

Personal data will be disclosed only to entities authorized under applicable law, in particular competent public authorities where Follow-up Actions are undertaken in connection with a reported Breach and in accordance with GPW's Whistleblower Protection Procedure.

Personal data may also be entrusted to service providers acting on behalf of GPW, such as IT service providers.

## **6. Source of Personal Data**

Your personal data were provided by the Whistleblower.

## **7. Retention Period**

Personal data will be processed for:

- 1)** Three years following the end of the calendar year in which Follow-up Actions were completed or proceedings initiated by those actions were concluded, in the case of Reports submitted under the Act.
- 2)** Five years, counted from the first day of the year following the year in which documents or information carriers were created or received and, in the case of internal rules, procedures, and other internal regulations, from the first day of the year following the year in which they ceased to apply, where the Report was submitted under the financial-market or AML regulations referred to above.

## **8. Right of Access**

You have the right to access your personal data, except that Article 15(1)(g) GDPR concerning information about the source of personal data shall not apply unless:

- the Whistleblower does not meet the conditions specified in Article 6 of the Act; or
- the Whistleblower has expressly consented to disclosure of their identity.

## **9. Other Rights**

You have the right to:

- rectify personal data;
- request erasure where permitted by law;
- request restriction of processing.

## **10. Right to Lodge a Complaint**

You have the right to lodge a complaint with the President of the Personal Data Protection Office if you believe that the processing of your personal data violates the GDPR.

## **11. Automated Decision-Making**

## Whistleblowing and Whistleblower Protection Procedure

Personal data will not be subject to profiling and no automated decision-making will be carried out on the basis of such data.