**Notification on the Protection of Personal Data When Submitting Reports on Violations**

**General Information about the Data Controller**

Data controllers and obligated parties under Art. 12, para. 1, item 3 of the Protection of Persons Who Report or Publicly Disclose Information on Breaches Act (PPWRPDIBA) are:

**Eleven Investments KDA, UIC 205173314**, with an address in Sofia, 31 Alexander Malinov Blvd., Campus X, Building 1, **and**

**ELEVEN PARTNERS AD, UIC 206322469**, with an address in Sofia, 31 Alexander Malinov Blvd., Campus X, Building 1,

**collectively referred to below as the "Controller/s"**

**I. What is the purpose of this Notification?**

The purpose of this Notification is to inform all individuals whose personal data is collected through the **internal whistleblowing system** about how their personal data is processed by the Controller when reporting violations.

Any processing of personal data carried out under the PPWRPDIBA, including exchange and/or transmission of personal data, is done in accordance with Regulation (EU) 2016/679 (the GDPR) and the Personal Data Protection Act.

**This Notification applies to:**
- The reporting person (whistleblower);
- All affected persons.

**II. Where is the personal data collected from?**

The Controller collects personal data provided by the whistleblower (the reporting person) through the internal reporting channel for violations. Furthermore, during the investigation of the report, personal data may be collected from other internal systems of the Controller and from third parties if necessary. The personal data concerning data subjects is collected directly from the data subjects when they submit a report using their name. The data concerning the data subjects may also be collected from sources other than the data subjects themselves, for example, when a report submitted by a data subject contains personal data about another person. During the processing of reports, the Controller may learn other personal data regarding the data subjects, which the whistleblowers voluntarily provide or which are obtained from other sources in a manner allowed or required by applicable law.

**III. Purpose and legal basis for processing**

**3.1. Purpose of processing**

We process your personal data for the following purpose: collection and processing of internal reports of violations with the purpose to comply with the PPWRPDIBA.

When you provide your personal data in a submitted report, we will collect and store your personal data in order to investigate your report and conduct an investigation. The information you provide will be kept strictly confidential and secure.

**3.2. Legal basis for processing**

The processing of personal data is lawful if any of the legal grounds specified in applicable law (Art. 6 of the GDPR) applies.

**We process personal data on the following legal grounds:**
• **Legal obligation**: We will process your personal data to fulfill our obligations under the PPWRPDIBA. The legal basis for this is Article 6 (1) (c) of the GDPR.

• If the information we receive in connection with a report of violations contains special categories of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health data, sexual life, sexual orientation of the individual, etc., the legal basis for processing such personal data is Article 9 (2) (g) of the GDPR, as processing is necessary for reasons of substantial public interest under EU and Bulgarian law.

• Data related to criminal offenses, convictions and security measures may be processed under the conditions specified in Article 10 of the GDPR and the Personal Data Protection Act.

**IV. Data subjects**

Under the GDPR, a data subject in connection with a submitted report may be:

● The author of the report (also referred to as the whistleblower or the reporting person);

● The person against whom the report is made and/or related persons (affected persons);

● The witness/witnesses and other persons whose personal data may become available during the investigation.

**V. What personal data do we collect?**

When you disclose information about violations (i.e., report possible wrongful actions), you are required to provide at least the following personal information:

● Your full name, address, phone number, and email address, if applicable;

● Your capacity as a whistleblower for a violation known to you in a work-related context – e.g., employee, contractor, freelancer, etc.;

● The name of the person against whom the report is made and their workplace, if the report concerns specific individuals and those individuals are known;

● Signature, electronic signature, and/or other identification of the reporter.

If necessary, we may request additional information to investigate all grounds for your report, together with any supporting documents or evidence.

**1. Categories of personal data that may be affected by the processing of the report:**

We acknowledge that the personal information in the violation report may relate to the whistleblower, the person against whom the report is made, witnesses of the violation, and/or other individuals mentioned in the report (affected persons).

Therefore, in connection with your submitted report, we will store and process the following personal data:

● Identity and contact information of witnesses;

● Identity, roles, and contact details of persons involved in the processing of the report;

● Information collected during the investigation of the reported facts;

● Information in reports generated during the investigation.

**2. Obligation for provision of your personal data:**

The processing of the personal data listed above is necessary to verify the information provided in the violation report. Failure to provide this data would prevent the processing of the report and the associated investigation.

Under the PPWRPDIBA, no proceedings are initiated for anonymous reports.

**VI. Who has access to the personal data and is the data disclosed to third parties?**

We take appropriate measures to protect the information related to submitted reports of violations and to safeguard the identity of whistleblowers, ensuring access to the information is granted only to employees who require it for the performance of their duties. Our goal is to ensure, as much as possible, the confidentiality of the information received and the protection of the identity of the whistleblower and all other involved persons.

The identity of the whistleblower is not disclosed to the persons against whom the accusations are made. **The identity of the whistleblower will only be disclosed if the whistleblower agrees** or **if the disclosure is required in criminal proceedings**, or **if the whistleblower has made a false report with malicious intent.**

Personal data may be disclosed to third parties, such as public authorities and/or external inspectors, when necessary and proportionate to meet a legal obligation imposed by Bulgarian law and/or EU law in the context of investigations by national authorities or judicial proceedings, including for the purpose of safeguarding the right of defense of the affected person. In these cases, before disclosing the identity and/or information related to the violation reports, we will notify the whistleblower about the necessity of disclosure. The notification will be written and substantiated. The whistleblower will not be notified when such notification could jeopardize the investigation and/or judicial proceedings.

## VII. Transfer of personal data outside the European Union/European Economic Area

The personal data received from a report is not transferred outside the EU or EEA.

## VIII. Retention period of personal data

Personal data will only be processed for the duration necessary to fulfill the obligations for which it was processed – in this case, to ensure compliance with the requirements for providing a reporting channel for violations. Personal data will not be processed for a period longer than necessary for the fulfillment of this purpose. Personal data irrelevant to the administration of the specific report will not be collected. If such data is collected by mistake, it will be deleted as soon as possible.

We are obliged to store reports and associated materials, including subsequent documentation related to their review for a period of 5 (five) years after the conclusion of the report review, unless criminal, civil, labor, or administrative proceedings are initiated in connection with the submitted report.

**We apply the following retention periods:**

| The report does not refer to this procedure | The report did not lead to any consequences | Where disciplinary or judicial proceedings have been initiated |
|---|---|---|
| The data is destroyed immediately | The data shall be destroyed within 5 (five) years after the conclusion of the examination of the report | The data shall be destroyed at the end of the procedure or the limitation period for appealing the decision |

After the retention period, the personal data shall be destroyed or anonymised. In the latter case, this means that it will be impossible to identify you by these data.

## IX. How do we ensure the safety and security of your information?

We have implemented technical and organizational measures to protect your personal data and take reasonable steps to safeguard your data from loss, misuse, unauthorized access, disclosure, alteration, or destruction.

We manage, maintain, and protect all information in accordance with the law, our policies, and best practices. All information is stored, processed, and transmitted securely. Access to personal data is strictly controlled.

We provide training to staff working with personal data, including on how to report security violations of the whistleblower's or other involved persons' personal data.

## X. Confidentiality

We will keep your identity confidential unless we are required to disclose it by law or receive your explicit consent.

We will notify you if we need to disclose your identity to investigating authorities.

**XI. What rights do you have as a data subject?**

Under GDPR, you have the following rights:

● *Right of access*: You have access to the personal data we store about you;
● *Right of rectification*: You may request us to correct any inaccurate or incomplete data;
● *Right of erasure (right to be forgotten)*: You may, under certain conditions, request that we erase your personal data. However, we may not comply with your request if we need your data to fulfill a legal obligation;

● *Right to restrict processing*, particularly if you dispute the accuracy of the personal data we store about you;

● *Right to object:* You may object to the processing of data that concerns you, based on a specific situation or specific circumstances regarding you.

To exercise the above rights or for any questions regarding personal data, please send a request to the Data Protection Officer at the following email: hello@11.vc.

If you believe the processing of your personal data violates the GDPR and the Personal Data Protection Act, you have the right to file a complaint with the supervisory authority - the Commission for Personal Data Protection, https://www.cpdp.bg/.