Privacy Notice for Whistleblowers
General information about the personal data controller

Administrator of personal data and obligated person under Art. 12, para. 1, item 3 of the Law on the Protection of Persons Submitting Whistleblowers or Publicly Disclosing Information on Violations:

" PayMan Group" OOD, EIK 206457036, with headquarters and management address in the city of Sofia, "Bulgaria" Blvd. No. 102, fl. 3, apartment office 26

I. What is the purpose of this Notice?

This notice purpose is to inform all individuals whose personal data are collected through **the internal whistleblowing system** about the manner and procedure for processing personal data by the administrator when reporting violations.

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

This Notice applies to:

- the reporting person.
- all affected persons.

II. Where is personal data collected from?

The administrator collects personal data provided by the whistleblower (the reporting person) through the internal channel for reporting violations. In addition, during the investigation of the report, if necessary, personal data is collected from the other internal systems of the administrator, as well as from third parties. Personal data concerning data subjects is collected from the data subjects themselves when they have reported using their name. Data about 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 the reports, the administrator may also learn other data about the data subjects that the reporters themselves voluntarily provide or that are obtained from other sources in a manner permitted or required by applicable law.

III. Purposes and 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 in order to comply with the Law on the Protection of Persons Submitting Whistleblowers or Publicly Disclosing Information on Violations .

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

3.2. Basis for processing

The processing of personal data is lawful if one of the legal grounds specified in the applicable law is present (Article 6 of the GDPR).

We process personal data on the following grounds:

- **Legal obligation:** We will process your personal data in order to fulfill our obligations under the Law on the Protection of Persons Submitting Whistleblowers or Publicly Disclosing Information on Violations. The legal basis we refer to is Article 6, paragraph 1, letter "c" of the GDPR.
- If the information we receive in connection with the report of violations contains a special category of data revealing the racial or ethnic origin, political views, religious and/or philosophical beliefs, data on the state of health, sex life, sexual orientation of the natural person, etc. n., the legal basis on which we will process these personal data is Article 9, paragraph 2, letter g) of the GDPR, because the processing is necessary for reasons of important public interest based on the law of the Union and Bulgarian law.
- Data related to crimes, 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

In the sense of the GDPR, a data subject in relation to the submitted report can be:

- the author of the report (also referred to as the whistleblower);
- the person against whom the report is filed and/or related persons (affected persons);
- the witness(es) and other persons whose personal data could become known in the course of the inspection.

V. What personal data do we collect?

When disclosing information about violations (i.e. reporting possible wrongdoing), you are asked to provide at least the following personal information:

- your three names, address and phone number, as well as an email address, if any;
- your capacity as a reporting person, for a violation that became known to you in a work context - worker, employee, self-employed, etc.;
- the names of the person against whom the report is filed and his workplace, if the report is filed against specific persons and they are known;
- signature, electronic signature and/or other identification of the sender.
- If necessary, we may request additional information so that we can investigate all the grounds for your report, along with any supporting documents or evidence.

1. The categories of personal data that may be affected by the processing of the signal:

We recognize that personal information in a whistleblower report may relate to the whistleblower (s), the person that is reported, witnesses to the breach and/or other individuals named in the whistleblower (data subjects).

Therefore, in connection with your report, we will also store the following personal information:

- identity and contact details of witnesses;

- identity, functions and contact details of the persons involved in the processing of the signal;
- information collected in the context of verifying the reported facts;
- information in reports prepared during the investigation.

2. Obligation to provide your personal data:

The processing of the above-mentioned personal data is necessary for the verification of the information indicated in the report of violations. Failure to provide this data would not allow the processing of the report and the conduct of the related investigation.

According to the Law on the Protection of Persons Submitting Whistleblowers or Publicly Disclosing Information on Violations, proceedings are not initiated based on anonymous reports.

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

We take appropriate measures to protect information related to reported violations and to protect the identity of whistleblowers, providing access to the information only to employees who need this data to perform their duties. It is our aim at all times to ensure, as far as possible, the confidentiality of the information received and the protection of the identity of the whistleblower and all other persons involved.

The identity of the whistleblower is not disclosed to the individuals against whom the allegations are made. **The whistleblower's identity is disclosed only if the whistleblower consents to it,** or **if disclosure of the whistleblower's identity is required in a criminal proceeding,** or **if the whistleblower has filed a false report with malicious intent.**

Personal data may be disclosed to third parties, such as public authorities and/or external inspectors, when this is a necessary and proportionate obligation imposed by Bulgarian law and/or European Union law in the context of investigations by national authorities or judicial proceedings, including with a view to guaranteeing the right of defense of the affected person. In these cases, prior to disclosing the identity and/or information related to the reported violations, we will notify the whistleblower of the need for disclosure. The notification shall be in writing and shall be motivated. The whistleblower is not notified when the investigation and/or legal proceedings are jeopardized.

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

Personal data obtained when reporting is not transferred outside the EU or EEA.

VIII. Period of storage of personal data

Personal data will only be processed to fulfill the obligations on which the processing is based – in this case to comply with the requirement to provide a breach reporting channel. Personal data will not be processed for a longer period than is necessary to fulfill this purpose. No personal data is collected that is clearly not relevant to the administration of the particular alert. If such data is collected in error, it will be deleted as soon as possible.

We are obliged to store the signals, and the materials attached to them, including the subsequent documentation related to their consideration, for a period of 5 (five) years after the conclusion of the

consideration of the report, except in the presence of criminal, civil, labor law and/or administrative proceedings in connection with the reported signal.

We apply the following storage periods:

The alert does not apply to this procedure	The alert did not lead to any consequences	When disciplinary or legal proceedings have been initiated
The data is destroyed immediately	The data is destroyed within 5 (five) years after completion of the examination of the signal	The data is destroyed at the end of the procedure or the limitation period for appealing the decision

After the storage period expires, personal data is destroyed or anonymized . In the latter case, this means that it will be impossible to identify you from this data.

IX. How do we ensure safety and security for your information?

We have implemented technical and organizational measures to protect your personal data and take reasonable steps to protect your data from loss, misuse, unauthorized access, disclosure, modification 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 in a secure manner. Access to all personal information is strictly controlled.

We provide training to staff who handle personal information, including how to report breaches of personal data to the whistleblower or others involved.

X. Confidentiality

We will keep your identity confidential unless we are required to disclose it by Law or we obtain your express consent.

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

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

According to GDPR, you have the following rights:

- *Right of access:* you have access to the personal data we store about you;
- *Right to rectification:* you can ask us to correct data that is inaccurate or incomplete;
- *Right to erasure* (right to be forgotten): you have the option, under certain conditions, to have the personal data we hold about you deleted. However, we have the option not to respond positively to your request, especially in the event that we need your data personal data to fulfill a legal obligation;
-

- *Right to restriction of processing* , in particular in case you dispute the accuracy of the personal data we store about you;
- *Right to object:* you can object, for reasons related to your specific situation and under certain conditions, to the processing of data concerning 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 address: **whistleblowing@mrpayman.com** .

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