Privacy notice on the processing of personal data regarding signals for breaches

Last Update 12.04.2024

"KPMG IT Service" OOD, UIC: 203572873, with headquarters and address of management: Sofia 1404, Blvd. Bulgaria No. 45/A ("KPMG ITS" or the "Company") is committed to protecting the confidentiality and inviolability of the personal data it collects and processes.

KPMG ITS is a liable person under the Law on the protection of persons who report or publicly disclose information on breaches ("LPPWRPDIB") and has established a channel for internal reporting of violations in accordance with the requirements of that Act.

With this document, we provide you with information on how KPMG ITS, as a personal data administrator within the meaning of the General Data Protection Regulation, collects, processes, stores or otherwise uses the personal data it receives in connection with reports of violations under the LPPWRPDIB.

1. What categories of data do we collect?

In connection with received signals for violations submitted under the LPPWRPDIB, we may collect and process the following categories of data:

- Three names, address, telephone, and e-mail address of the sender of the signal, as well as the classification of the sender.
- The names of the person against whom the signal is filed and his/her place of work if the alert is filed against specific persons and they are known.
- Specific data of a breach or of a real danger of such a breach, place, and period of the breach, if one has been committed, a description of the act or situation and other circumstances, to the extent indicated by the reporting person, or collected during the internal review of the signal.
- Signature, electronic signature or other identification of the sender of the signal.
- Other data, including from any kind of sources of information, contained or collected in connection with the specific signal.

KPMG ITS does not collect or process data that manifestly does not relate to the signal and/or does not contribute to clarifying the facts and circumstances of the reported breach or is otherwise manifestly irrelevant to the consideration of a specific signal. In the event that such data is obtained or collected accidentally, it will be deleted or destroyed by the Company, or returned to the person who provided them without undue delay, but not later than one month from their receipt.

2. How do we collect your personal data?

- Directly: We may receive personal data directly from you when you are a whistleblower or if you participate in the inspection of a signal as an affected person, witness or other capacity and provide us with your personal data.
- Indirectly: We may receive information about you listed in a report of a breach filed by another person, or during an internal review of such a signal.

3. For what purpose do we collect and process your personal data?

In connection with received signals for violations under the LPPWRPDIB, KPMG ITS collects and processes personal data for the following purposes:

- Registration and administration of received signals.
- Internal verification of the received signals.
- Maintaining contact with the person who submitted the signal, including providing feedback on a signal.

- Making contact with the persons indicated in the received signals.
- Detection, prevention and cessation of violations.
- Adoption of follow-up actions in relation to detected violations.
- Providing protection to the whistleblower, persons associated with the whistleblower, and the affected person in cases under the LPPWRPDIB.
- Compliance with legal obligations applicable to the Company.

4. On what basis are we collecting and processing your personal data?

KPMG ITS collects and processes personal data in connection with received signals for violations covered by the LPPWRPDIB, in the course of internal checks on such signals and when taking subsequent actions on them on the basis of compliance with the legal obligations provided for in the LPPWRPDIB that apply to the Company.

In the event that a signal contains special categories of personal data or if, in the course of the internal check, KPMG ITS receives such data, their processing shall be carried out insofar as there is a basis for processing under Article 9(2) of the General Data Protection Regulation. In case there is no basis for processing of the collected personal data KPMG ITS will erase or destroy them without undue delay, but no later than one month from their receipt.

5. Are you obliged to provide us with your personal data?

The provision of the aforementioned personal data to the whistleblower is a legal requirement provided for in the HIPAA and is necessary for the examination of the submitted signal under the terms and conditions of the said law. If you do not provide us with sufficient information, we may not be able to investigate the tip received or conduct an internal investigation into it or provide feedback on the results of the investigation and the action taken.

6. Who can access your personal data?

Within KPMG ITS, access to personal data collected and processed in connection with received signals for violations is provided only to employees who need them for the performance of their duties, including the Whistleblowing Officer and their deputy insofar as they are not affected by the signal. In the event of identified breaches, the Company's Managing Directors and other responsible employees within the organization may be given access to information relating to a specific breach and its perpetrator, if necessary, in order to take further action.
Outside the Company, personal data related to a specific signal may be provided to the competent authorities in accordance with the applicable legislation, as well as to professional advisers, lawyers and insurers of the Company under the obligation to maintain confidentiality and in compliance with the requirements of the LPPWRPDIB.

7. Do we transfer your personal data outside the European Economic Area?

Personal data received in connection with signals and in the course of internal checks on them will be processed and stored on the territory of the European Union and will not be transferred to third countries or international organizations.

8. How long do we keep your personal data?

KPMG ITS stores the personal data it collects and processes in connection with received signals for violations for a period of 5 (five) years from the date of completion of the internal verification of the signal, and in case no internal verification has been carried out (for example, if the report is forwarded under the competence of the relevant authority or returned to the reporting person due to irregularity) – 5 (five) years, from the date the forwarding of the signal or the date of the written decision that the internal review of the alert will not be carried out.

Storage of data for a longer period is exceptionally allowed in case of criminal, civil, labour and/or administrative proceedings, and in such cases the data shall be retained until the final conclusion of the

proceedings and for a period of five (5) years thereafter, for the purpose of establishing, exercising or defending legal claims.

9. What are your rights under data protection legislation and how can you exercise them?

The General Data Protection Regulation guarantees you a certain set of rights that you can exercise with respect to the personal data we process when the prerequisites for this are met. The Regulation grants you the following rights:

- Access – You may require us to confirm whether we process your personal data and, if so, to provide you with detailed information in this regard.
- Correction – You may require us to correct our records containing personal data if you believe they are inaccurate, outdated or incomplete.
- Deletion ("right to be forgotten") – You may ask us to delete your personal data when they are no longer necessary for the purposes for which they were originally collected and processed, when the personal data have been unlawfully processed, and when the personal data must be erased in order to comply with a legal obligation to which the Company is subject.
- Restriction of processing – You may require us to temporarily restrict the processing of your personal data if you contest their accuracy, you prefer to restrict the processing of the data instead of asking us to delete it or you want us to keep it for you for the purpose of establishing, exercising or defending legal claims. It is possible that we temporarily stop the processing of your personal data until we establish whether we have overriding legitimate grounds for processing them.

Each of these rights may be exercised to the extent that it is applicable and in the presence of the required legal prerequisites for doing so.

You can exercise your rights by sending an application to: Sofia 1766, Mladost 4, Business Park Sofia, building 15A, floor 3, or by sending us an email to: de-dlitsooddataprivacy@kpmg.de. Before complying with your request to exercise a right, we may ask for additional information to verify your identity.

If you believe that KPMG ITS has violated any of your rights in relation to the protection of personal data, you have the right to file a complaint with the Personal Data Protection Commission of the Republic of Bulgaria.

10. Do we change this Personal Data Processing Privacy Notice?

In cases where we make changes to this Privacy Notice, we will indicate the date of the last update at the beginning of this document. Any changes in relation to the processing of personal data that affect you and are described in this Notice will be brought to your knowledge in an appropriate manner, depending on how we normally communicate with you.