Information about the terms and conditions for reporting of breaches

Last Updated 27. 04. 2023

KPMG IT Service OOD, UIC 203572873 ("KPMG ITS" or the "Company") is committed to complying with all laws and regulations applicable to the Company.

In order to ensure compliance with regulatory requirements, among other things, it is important for the Company to obtain timely information about possible misconduct of an employee or supplier and thus be able to take appropriate action to terminate this. For this reason, and in pursuance of the Law on the Protection of Persons Who Report or Publicly Disclose Information on Breaches ("LPPWRPDIB"), the Company has established a channel for internal reporting of breaches.

How can you report a violation?

Reports of breaches can be submitted through the following channels:

- In writing - by e-mail to the following e-mail address: de-fmitsoodsignals@kpmg.de
- Verbally – through a personal meeting with the Officer responsible for handling signals.

The officer responsible for handling signals of KPMG ITS is Mrs. Katerina Georgieva. You can contact Mrs. Georgieva to arrange a personal meeting to report violations by phone: +49 30 2068 3627 or by writing to the following email address: de-fmitsoodsignals@kpmg.de.

What should the signal contain?

When submitting a written report, please use the signal registration form, which can be downloaded here: https://kpmg-its.bg/ whistleblowing/ , as well as to be provided at request by the Officer responsible for handling signals using the contact details listed above.

According to the requirements of the LPPWRPDIB, your signal should contain at least the following data:

- The full name, address and telephone number of the sender, as well as an e-mail address, if any.
- The names of the person against whom the signal is made and his/her place of work, if the signal is filed against specific persons and they are known.
- Specific data on a breach or a real danger of such a breach, place and period of the breach, if one has occurred, a description of the act or situation and other circumstances, to the extent known to the reporting person.
- Date of the signal.
- Signature, electronic signature or other identification of the sender.

The signal may be accompanied by any kind of information supporting the allegations made therein and/or reference to documents, including the indication of data on persons who could confirm the data communicated or provide additional information.

What breaches can be reported?

Through the above channels, you can report the following breaches, which are known to you in a working context:

- Violations in the field of:
  - Procurement;
  - financial services, products and markets and the prevention of money laundering and terrorist financing;
  - the safety and conformity of products;
  - transport safety;
  - environmental protection;
  - radiation protection and nuclear safety;
  - food and feed safety, animal health and welfare;
  - public health;
  - consumer protection;
  - the protection of privacy and personal data;
  - the security of network and information systems;
- Infringements affecting the financial interests of the European Union.
- Infringements of internal market rules, including European Union rules and Bulgarian competition and State aid legislation.
- Infringements relating to cross-border tax schemes the purpose of which is to obtain a tax advantage which is contrary to the object or purpose of the applicable corporate tax law.
- A crime of a general nature has been committed, of which you have become aware in connection with the performance of your work or in the performance of your duties.
- Violations of the Bulgarian legislation in the field of:
  - the rules for payment of due public state and municipal receivables;
  - labour law;
  - legislation relating to the performance of a civil service.

In which cases will your signal not be considered?

The Company will not consider the following signals:

- Signals that do not relate to breaches within the above scope and therefore do not fall within the scope of the LPPWRPDIB.
- The content of the alert does not justify its acceptance as plausible.
- Reports that are submitted anonymously.
- Reports relating to breaches committed more than two years ago as from the date of reporting.
- Signals that do not meet the legal requirements and the irregularities are not eliminated within 7 days.

- The signal contains obviously false or misleading statements of facts and these allegations have not been corrected by the whistleblower.

How does the Company protect your rights when reporting a breach?

The Company examines all reports of violations in compliance with the principles of confidentiality, impartiality, fairness, independence and lack of conflict of interest.

KPMG ITS protects the information related to the reported breaches, including but not limited to the identity of the whistleblower and other persons identified in the report or made aware of the report.

Access to information related to reported breaches is strictly limited only to employees to whom this data is necessary for the performance of their duties.

The Company shall protect reporting persons from retaliatory acts having the character of repression and placing them at a disadvantage and shall not allow such actions to be carried out within its organisation.

According to the requirements of the LPPWRPDIB, protection is granted to the person reporting breaches through an internal channel, provided that the reporting person had reasonable grounds to believe that the information submitted about the breach in the report was correct at the time of its submission and that this information falls within the scope of the LPPWRPDIB referred to above and has reported a violation under the terms and conditions of the LPPWRPDIB.

To the extent applicable to the Company, the protection shall be provided to a natural person who reports an infringement that has become known to him/her in their capacity as:

- a worker, employee, civil servant or other person performing hired labor, regardless of the nature of the work, the method of payment and the source of the funding;
- a person who performs work without an employment relationship, a freelancer and/or craftsman;
- volunteer or trainee;
- partner, shareholder, sole owner of the capital, member of the management or control body, member of the audit committee of an enterprise;
- a person who works for a natural or legal person, its subcontractors or suppliers;
- a candidate for employment who has participated in a contest or other form of selection for employment and has received information about an infringement in that capacity;
- an employee, where the information was obtained in the context of an employment relationship which was terminated at the time of reporting or public disclosure;
- any other person reporting a breach that has become known to him or her in a working context.

Protection shall also be granted to:

- persons assisting the reporting person in the reporting process;

- persons who are related to the reporting person (such as colleagues or relatives) and who may be subject to retaliatory response due to the reporting;
- legal persons in which the reporting person holds a holding, for which he or she works or is otherwise related in a working context.

How can you report a signal to the central authority handling such signals?

The Central Authority for External Reporting of Violations under the LPPWRPDIB is the Commission for Personal Data Protection of the Republic of Bulgaria.

More information about the procedures for external reporting can be found on the website of the Commission for Personal Data Protection: https://www.cpdp.bg/.