

Information about the terms and conditions for reporting of breaches

Last Updated 12.04.2024

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.

1. Who can report a breach?

You can report a breach through the KPMG ITS internal whistleblowing channel if you are a whistleblower within the meaning of LPPWRPDIB, namely an individual who reports a breach of which they have knowledge in a work context, in their capacity as:

- current or former employee of KPMG ITS;
- Manager of KPMG ITS;
- A person who works without an employment relationship with KPMG ITS, including a freelancer engaged by KPMG ITS;
- A volunteer (paid or unpaid) or intern at KPMG ITS;
- A contractor, subcontractor or supplier of KPMG ITS, and their employees;
- A person whose employment relationship with KPMG ITS is about to commence in cases where information concerning the violation was obtained during the recruitment process or other pre-contractual relationship;
- Any other person provided for in the LPPWRPDIB, to the extent applicable to KPMG ITS.

2. What violations can be reported?

You can report the following violations related to the activities of KPMG ITS that you have become aware of in a work context:

- Violations in the area of:
 - Privacy and data protection;
 - security of networks and information systems;
 - environmental protection;
- Offences relating to cross-border tax schemes designed to obtain a tax advantage contrary to the object or purpose of applicable corporate tax law.
- An offence of a general nature of which you have become aware in connection with the performance of your work or in the course of your duties.
- Violations of Bulgarian law in the area of rules on payment of public state and municipal claims or employment law.
- Other breaches referred to in the LPPWRPDIB.

3. 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 Whistleblowing Officer of KPMG ITS is Mrs. Radka Chamova. You can contact Mrs. Chamova to arrange a personal meeting to report violations by phone: +49 30 2068 1127 or by writing to the following email address: de-fmitsoodsignals@kpmg.de.

In case your signal concerns the Whistleblowing Officer, or in case of his/her absence you can submit your signal to Mrs. Maria Konstantinova. You can contact Mrs. Konstantinova to arrange a personal meeting to report violations by phone: +49 30 2068 4742 or by writing to the following email address: mconstantinova@kpmg.com.

4. What should the signal contain?

When submitting a written report, you can 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 Whistleblowing Officer or his/her deputy 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, as well as well as the classification of the sender.
- 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.

5. 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 scope of the LPPWRPDIB.
- Signals whose content does not warrant being considered plausible.
- Signals that are submitted anonymously.
- Signals 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.
- Signals which contain obviously false or misleading statements of facts and these allegations have not been corrected by the whistleblower.

6. 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, subject to a commitment to confidentiality.

The Company shall protect reporting persons from retaliatory acts having the character of repression and placing them at a disadvantage, as well as threats or attempts to do so, and shall not allow such actions to be carried out within its organization.

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 and has reported a violation under the terms and conditions of the LPPWRPDIB.

Protection under the LPPWRPDIB is also afforded to persons who assist the whistleblower in the whistleblowing process and whose assistance should be confidential, persons who are related through work or relatives of the whistleblower and may be subject to retaliation for whistleblowing, and legal entities in which the whistleblower has an ownership interest, works for, or is otherwise associated with in a work context.

The whistleblower shall be liable if it knowingly made a false report.

7. 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.cdpd.bg/>.