Information about processing of personal data for the whistleblower service

KPMG AMO Whistleblower Service

1 Background

KPMG AB (“KPMG”) has created this Information about processing of personal data for the whistleblower service to accompany the information text. These two information texts serve as the foundation for the information that organizations using KPMG's Whistleblower Service must provide to registered individuals in compliance with the regulations governing personal data processing.

Organizations may need to adapt this information to ensure its comprehensiveness. The client bears the responsibility for updating this information as needed.

Under the General Data Protection Regulation (GDPR), there is an obligation to provide information to data subjects in two situations: when information is collected directly from the data subject (Article 13) and when personal data is obtained indirectly (Article 14). This information text addresses both scenarios.

With regard to persons to whom the reporting relates, exceptions from the obligation to inform these persons may exist, but it is advisable to maintain a general description accessible, such as on the organization's website or intranet.

2 Information for reporting persons and others than reporting persons

2.1 Personal data controller

The personal data controller for the processing of personal data in connection with the reporting of irregularities is SSC. Contact information and information about representatives is available on SSC’s website.

2.2 General information on the handling of personal data after reporting in the whistleblower channel

Reporting individuals submit their reports through KPMG's web application or via voicemail. A designated KPMG employee is assigned to the case and can then review the report.

Only the employee or employees assigned to a case within the reporting system have access to review and correspond with the reporting individual.

The reporting person can choose to remain anonymous However, choosing to do so may make it more challenging to follow up on the information provided.

There is a messaging feature within the web application. When reporting persons write messages in a reported case, the case manager only sees the case reference number of the sender.

Upon receiving a report, an initial assessment is conducted to evaluate the information and determine whether additional details are required. KPMG will then provide a Possible actions may include:

- Closing the case (e.g., due to insufficient evidence or other reasons).
- Initiating a thorough investigation.
- Forwarding the case for internal or external handling (e.g., to the Legal department or law enforcement authorities).

We encourage reporters to provide only relevant information related to the case, and to avoid deliberately providing false statements or content that may be perceived as offensive.

2.3 Purpose of the processing of personal data

The purpose of processing personal data in connection with the handling of whistleblower cases is twofold. Firstly, SSC aims to prevent, detect, and remedy misconduct within the business and in certain instances, to establish, assert, or defend legal claims arising from reported misconduct.

Secondly, the processing of personal data also serves the purpose of enabling SSC to fulfil its obligations as mandated by applicable regulations governing the reporting of malpractice, including the Protection of Persons Who Report Malpractice Act (2021:890)

2.4 Legal basis for the processing of personal data

The legal basis for the processing of personal data in internal and external is the necessity to fulfil legal obligations imposed on the data controller. These legal obligations are specified in the law on the protection of individuals who report malpractice.

2.5 The recipient of personal data

Reporting through the whistleblower service is managed by KPMG, using a system provided by KPMG. The information stored in the system remains within Sweden and is handled by specially designated employees at KPMG on behalf of the data controller.

Furthermore, information, including personal data, may be disclosed to individuals specified by the data controller, law enforcement agencies such as the police or prosecutors, or other relevant authorities. The decision to disclose information depends on the specific circumstances of each case. This includes considerations such as whether it is relevant to initiate personnel proceedings or if reporting to the police is warranted due to the nature of the report.

2.6 Storage of personal data

Personal data collected for the management of whistleblower cases will be retained for a maximum of two years following the conclusion of data processing in the respective case.

A reporting case is considered closed when the whistleblower function has taken final actions in the case. This includes instances such as when the data controller decides to close an investigation, pass the information for further examination or handling, or when legal proceedings related to the case have concluded.

2.7 Categories of personal data

The categories of personal data that may be processed in the context of a whistleblower case depend on what information is provided by the reporting person and on what information needs to be obtained from other people or sources of information, for example to investigate or verify the information provided by a reporting person.

The following categories of personal data may be processed in the context of a whistleblower case:

- Contact details,
- Social security number / coordination number,
- Information on employment, e.g., position,
- Income information, including salary and other benefits, income from capital, and business activities,
- Information on assets and investments such as account numbers, bank account holdings, holdings of securities and real estate, etc.,
- Membership in a trade union,
- Sexual orientation (e.g., when reporting discrimination),
- Religious or philosophical beliefs (e.g., when reporting discrimination),
- Racial or ethnic origin (e.g., when reporting discrimination),
- Political opinions (e.g., when reporting on discrimination),
- Information on the sexual life of a natural person (e.g., when reporting harassment or abuse),
- Health information and
- suspected or established breaches of rules.

Given that the person responsible for personal data does not control what information is provided in the reporting channel, it is not certain that the above list is completely exhaustive.

2.8 Origin of the data

Personal data for the handling of whistleblower cases is collected from persons who report cases through the whistleblower channel and may also be collected from:

- Other persons who may be contacted because they are deemed to have relevant information about the case,
- Publicly available sources such as search services,
- Social media and
- Authorities such as the Swedish Tax Agency, the Swedish Enforcement Authority, and courts.

2.9 Rights of data subjects

Registered persons have certain rights, subject to restrictions and exceptions, which include the following:

- The right to access personal data processed about them.
- The right to request the correction of inaccurate personal data and the addition of missing and relevant data for the processing's purpose.
- The right to request the deletion of their personal data.
- The right to request the restriction of processing their personal data.
- The right to request access to and the transfer of their personal data to another controller (data portability), with the receiving controller obligated to facilitate such transfer.
- The right to object to the processing of their personal data by the data controller. This right applies, among other instances, to personal data processed after a balance of interests and includes the right to object to profiling

A request for the exercise of any of the above rights shall be sent to Swedish Space Corporation’s Data Protection Officer

The person whose personal data is processed also has the right to report complaints to the Swedish Authority for Privacy Protection. See information about this on the Swedish Authority for Privacy Protection's website.