Practice Name:

Whistle-Blower tool

Country:

Austria

Practice category:

- Systems and tools

Contact:

- Public Prosecutor's Office for Combatting Economic Crime and Corruption
- www.justiz.gv.at/wksta/
- +43 1 526 36 86

Fraud risk(s) countered

- Conflict of interest
- Avoidance or manipulation of public procurement procedures
- Double funding
- Collusion
- Manipulation of project costs
- Others

Context and objective(s)

The Austrian Public Prosecutor's Office for Combatting Economic Crimes and Corruption (PPO) launched an anonymous whistle-blower tool in 2013 as part of the fight against corruption. The tool includes a mailbox which allows communication with the whistle-blower to ask for further clarification. After an initial trial phase, the system has been permanently established since 2016 and a paragraph about the system and its mandate was added to the law (§ 2a Abs 6 StAG).

Criminal structures can often only be exposed if the reporting whistle-blower is sufficiently protected from negative consequences. The whistle-blower tool ensures the anonymity of the whistle-blower and shall increase the reporting of economic crimes.

The aim of the tool is to enable investigators of the PPO to get in direct contact with whistle-blowers. This increases the effectiveness of prosecuting crimes.

Description of the practice

The tool is set up as an anonymous email system using the BKMS System by Business Keeper (**https://www.business-keeper.com/**) which is one of the leading providers of whistleblowing systems in the EU.

It invites citizens to report suspicious observations in their work or private environment via a link on the website of the Federal Ministry of Justice. The technical implementation of the system guarantees that the source of the submission cannot be traced. Whistle-blowers are entitled to decide whether they would like to remain anonymous or to identify themselves to the investigators.

If the investigators have additional questions based on the submitted information, they can contact the whistle-blower directly via a mailbox in the tool. The identity of the whistle-blower remains protected throughout the process.

Contrary to receiving anonymous information via post or through other channels, the prosecutors now have the option to ask for further information which can be used to corroborate the allegations and potentially open an investigation.

There are several specific categories under which information can be submitted, in accordance with Austria's Criminal Code:

- Corruption,
- Financial Crime,
- Welfare Fraud,
- Fraudulent Accounting,
- Capital-Market Offences, and
- Money Laundering.

The reporting process follows these 4 steps. The reporting person:

1. Is required to read information relating to the protection of his/her identity,
2. Chooses the main category of his/her report from a list containing Corruption, Financial Crime, Welfare Fraud, Fraudulent Accounting or Capital-Market-Offences and Money Laundering;
3. Describes the case in his/her own words and answers a set of predefined questions, e.g. relating to the damages incurred and the place of the incident; it is also possible to upload documents, and
4. Is asked to set up a mailbox to communicate with the investigators.

The setup of the mailbox is not required to submit a report, but rather it is optional after the first three steps listed above.

The whistle-blower is also asked specifically whether they want to remain anonymous. They can also opt to be treated as a key witness if they were involved in the crime being reported.

The person is reminded that the information and documents provided could lead to their identification and that special care is thus required, e.g. in choosing their pseudonym for the mailbox or by not disclosing their relationship to the accused in their description of the case. The tool specifically warns against using a work computer for reporting.

After submitting the report, the whistle-blower receives a reference number as confirmation of submission.

The report reaches the PPO where four specifically trained prosecutors currently deal with the incoming reports. On top of their expertise as prosecutors, the investigators received initial training by Business Keeper about the handling of the BKMS system and regularly take courses about relevant topics, e.g. communication with the whistle-blower.

When communicating with the whistle-blower, the investigators also remain anonymous to be equally protected.

Every report is assessed by two prosecutors to allow a 4-eyes-review. The PPO can define appropriate measures instantly or forward the report to another department if the report does not fall within its responsibility. If the report is deemed substantive, the PPO opens an investigation. In instances where the report does not represent a case that needs further action, the case is closed.
The whistle-blower is informed about the steps without receiving detailed information. Given that the identity of the whistle-blowers is not known, they might not be entitled to receive information about the investigation, e.g. regarding potential victims.

The BKMS system is also a case-management-system. All the communication and documents relevant to one report are securely and electronically stored within the system. If an investigation is opened, the relevant information can be easily forwarded.

The tool is being continuously improved, e.g. by adapting the information the whistle-blower is provided with and facilitating the use of the system for the investigators.

Unique features

- Anonymity of the whistle-blower
- Communication with the whistle-blower possible through a post-box in the system
- Encrypted communication
- Access only for the dedicated team within PPO; not the Business Keeper provider or other third parties
- Technical information about the whistle-blower, e.g. IP address, is not stored
- System is accessible 24/7 worldwide
- Whistle-blowers are reminded several times about not disclosing any information that could lead to their identification in the report, if they want to stay anonymous

Outcomes and results

Since the tool was launched, the perception of the Austrian judiciary's has changed significantly: accommodating and encouraging whistle-blowers has been recognised due to serious recent cases of corruption in Austria.

At the end of 2019, the website was visited more than 600 000 times, with approximately 300 accesses per day on average. 9345 reports were made and in 6210 cases the whistle-blower used the option to create a post-box for further communication.

679 investigations were initiated based on the reports received. 66 charges were brought to court; in 48 reports to the PPO the information received was novel. 93 reports were being used in ongoing proceedings.

Reports were made in the following categories:

- 17,02% Corruption,
- 19,45% Welfare Fraud,
- 16,82% Financial Crime,
- 22,21% Fiscal Crime,
- 0,62% Fraudulent Accounting and Capital-Market Offences, and
- 2,49% Money Laundering
- 21,39% were “other” cases which could not be categorised as one of the topics listed above.

Key success factors

- Ensuring anonymity for whistle-blowers
- Cooperation with experienced tool providers
- Training of prosecutors in charge of the reports
- Communication about the implementation of the tool in the media and on the website of the PPO

Challenges encountered & lessons learned

- Legal foundation, i.e. a paragraph in the law, is key to promoting reporting and guaranteeing that the information can be used in judicial proceedings
- Cooperation with well-established tool provider ensures secure handling of the data and structured management of the cases
- Appropriate communication about the existence and use of the tool as well as the handling of the information is crucial to encouraging reporting

Potential for the transferability

- A system from the same or a similar tool provider can be easily incorporated by other countries/authorities,
- Given the adoption of the Directive on the protection of persons reporting on breaches of Union law (also known as the Whistle-blower Directive) which requires all Member States to create a channel for reporting breaches, this practice might serve as guidance (the Directive needs to be transposed into national law by December 2021),
- Ensuring anonymity is not legally possible in all Member States.