INFORMATION

ON WHISTLEBLOWING AND THE PROTECTION OF WHISTLEBLOWERS

Why are whistleblowers important to us?

We see whistleblowing as an important feedback loop to improve our own organisation and processes and reduce our risks. It is therefore important for us to understand the risks associated with our operations and to protect and support whistleblowers in good faith. We support whistleblowing and protect whistleblowers in line with our Anti-Corruption Policy and our anti-corruption management system. No one should be disadvantaged for making a report in good faith.

What is the whistleblowing system?

Intelliport Systems Ltd. and Intelliport Solutions Ltd. (hereinafter referred to as "Intelliport") operate an integrated, joint internal whistleblowing system in accordance with our Anti-Corruption Policy and anti-corruption management system, which is designed to ensure that data and information about a risk or deficiency in Intelliport's operations that is brought to the attention of decision-makers by a whistleblower and, if necessary, to take action to address the risk.

Who can be a whistleblower?

A whistleblower may be an employee of Intelliport, a person who has a contractual relationship with Intelliport or a person who has a legitimate interest in making a whistleblower report. Intelliport expressly encourages whistleblowers to report to its whistleblowing system who are not named as whistleblowers in Act XXV of 2023 on the Rules on Complaints, Whistleblowing and Reporting Abuses of Public Interest.

What can be reported?

Any event, circumstance, occurrence, omission, defect or information that may pose a risk to the operation of Intelliport. In particular, serious breaches of organisational ethics and conduct, fraud, anti-competitive behaviour or money laundering may be reported. This includes, in particular, concerns about corruption, attempted or suspected corruption, or any breach or deficiency of the anti-corruption management system.

How to report?

You can make a report primarily by emailing compliance@intelliport.hu, but you can also do so by writing to the Compliance Officer or in person.

Can I report anonymously?

We store personal data of whistleblowers wo report in person data in a separate, sealed envelope. We will assess whistleblowing reports based on their content. We will also investigate a report made by an anonymous or unidentified whistleblower if its content is likely to reveal a risk relevant to the organisation's operations, but we encourage whistleblowers to provide their contact details to ensure feedback.

Who deals with the report?

A specially trained compliance officer is responsible for receiving, processing and investigating the report.

What happens with the report?

The compliance officer receives the report and sends an acknowledgement to the whistleblower within seven days of receipt of the report, providing general information on the internal investigation process and data management rules under Act XXV of 2023 on the Rules on Complaints, Whistleblowing and Reporting Abuses of Public Interest. The compliance officer will classify the whistleblowing report into a risk group (low, medium or high) based on its content and the presumed impact. If there is insufficient information available to classify the report into a risk group or to investigate the report, the whistleblower will be contacted using the contact details available. If the whistleblowing is low risk or easy to handle, the compliance officer will act at his/her discretion and notify the whistleblower within 7 days from the date of receipt of the whistleblowing, but no later than 30 days. If the report is in a medium or higher risk category and the substantiation of the allegations cannot be clearly established, the compliance officer will take action to investigate the allegations in the report.

What is being investigated in relation to the report?

The purpose of the investigation is to determine whether the data and information contained in the report is accurate and whether the organisation's risk reduction procedures are justified. The whistleblower will be informed of the start and progress of the investigation and, if necessary, will be asked to provide documents and other evidence to assist the investigation of the report, with a deadline. In the course of the investigation, the compliance officer may conduct interviews, obtain statements, seize documents, and inspect and make copies of data found on computers without compromising the integrity of the original data.

When can a whistleblowing have an effect?

The whistleblowing report will be investigated within the shortest time possible in the circumstances, but no later than 30 days from the date of receipt. In particularly justified cases, the time limit for the investigation may be extended, but may not exceed three months. If the investigation leading to an assessment is expected to take longer than 30 days, the whistleblower will be informed of this, together with the expected date of the assessment and the reasons for the extension.

What will be the consequences of the whistleblowing?

After the investigation is closed, the compliance officer will prepare a report on the outcome of the investigation, which will include a recommendation for a decision on further action. The compliance officer will send the report to the relevant manager of Intelliport. Based on the report, the manager will decide on further action and inform the compliance officer, who will notify the whistleblower.

What are the consequences of a false or malicious whisthleblowing?

The false or malicious whistleblower will be made aware of the consequences of his/her actions. Sanctions will be applied only in the most appropriate cases, which may be employment or contractual sanctions, commensurate with the seriousness of the offence and taking into account the circumstances of the whistleblowing. The compliance officer may propose any sanction.

Our data protection requirements

In handling whistleblowings, we comply with the applicable legislation and our own internal data protection rules, while fully respecting the principles of personal data protection, data security, purpose limitation and data integrity. We process personal data of the whistleblower and of the persons concerned by the notification (whose conduct or omission gave rise to the whistleblowing or who may have material information about the subject matter of the whistleblowing) which is necessary for the investigation of the whistleblowing, solely for the purposes of investigating the report and remedying or stopping the conduct that is the subject of the whistleblowing. Other personal data will be deleted from our systems without delay. We will not disclose the whistleblower's personal data without the prior written consent of the whistleblower. Data processed under the internal whistleblowing system will not be transferred to third countries or international organisations.

To whom do we disclose personal data related to the whistleblowing?

Only to those bodies to which we are legally obliged to do so. Therefore, personal data stored in the internal whistleblowing system will only be transferred to the body competent to carry out the procedure initiated on the basis of the whistleblowing, if that body is entitled to process it by law or if

the whistleblower has consented to the transfer of his/her data. An exception to this rule is where it has become apparent that the whistleblower has communicated false data or information in bad faith and where there are indications that a crime or an offence has been committed. In such a case, your personal data will be transferred to the body or person responsible for the procedure. We will act in the same way at the request of the body or person entitled to initiate or conduct the proceedings if there are reasonable grounds to believe that the whistleblower has caused unlawful damage or other harm to another person by his or her whistleblowing.

How do we protect personal data?

Our internal whistleblowing system is designed to ensure that the personal data of the whistleblower who discloses his or her identity and of the person concerned by the whistleblowing (including anyone who may have material information about the whistleblowing) cannot be disclosed to anyone other than the authorised person. Pending the conclusion of the investigation or the initiation of action as a result of the investigation, the person investigating the report will not share information about the content of the report and the individual subject of the report with any other Intelliport department or employee, other than the person subject of the report, except to the extent strictly necessary to conduct the investigation.

Rights of the person concerned by the whistleblowing

The person concerned by the whistleblowing will be informed in detail about the report, his or her rights regarding the protection of his or her personal data and the rules on the processing of his or her data when the investigation is opened by sending this information notice. In accordance with the requirement of a fair hearing, we will ensure that the person concerned can express his or her views on the whistleblowing, including through legal representation, and that these views are supported by evidence. Exceptionally, and in duly justified cases, the person concerned may be informed at a later stage if immediate information would prevent the investigation of the report.