Whistleblower Privacy Policy
IATS Management System

Document No.: D6990-082 Version: 01.00.00

Insero Air Traffic Solutions A/S
Banegårdsgade 2
8700 Horsens
Denmark

T +45 79 25 33 00
info@inseroats.com
https://inseroats.com/

CVR 66849716

Contents

Tables

Version History

Version	Date	Prep.	App.	Change Description
01.00.00	2024-12-12	MITA, CDL	ERBO	First release

Table 1: Version History

1. Introduction

1.1 Purpose

This document describes the privacy policy, including GDPR Article 30 Record, in relation to the Insero Air Traffic Solutions (IATS) Whistle Blower Policy and forms part of the IATS Management System.

1.2 Scope

This document applies to the IATS Whistle Blower Policy.

1.3 Responsibility

This document is maintained by the IATS Quality Manager and shall be approved by the IATS Chairman of the Board.

2. Whistle Blower Policy

2.1 The purpose and legal basis for the whistleblower scheme

The purpose is to make a whistleblower scheme available to the IATS staff and external stakeholders.

Basis for processing personal data:

- GDPR Article 6(1), point f (the legitimate interests rule) in that the organisation has a substantive interest in processing in-formation reported via a whistleblower scheme and this interest is deemed to carry more weight than the consideration for data subjects who may be mentioned in a report.

Exception to the prohibition on the processing of sensitive personal data and information on criminal convictions and offenses:

- GDPR Article 9(2), point f (necessary for the establishment, exercise or defence of legal claims).
- GDPR Article 9(2), point g (necessary for reasons of substantial public interest)
- GDPR Article 10 (processing of personal data relating to criminal convictions and offences).

2.2 Categorising of data subjects

- Employees
- Any whistleblowers who are not employees
- Persons who are the subject of a report
- Other partners, board members, etc.

2.3 Categorising of personal data

The information the whistleblower chooses to report to the whistle-blower scheme.

The whistleblower can choose to remain anonymous in connection with a report. The whistleblower may, however, choose to waive anonymity during the process, and a report concerning other identifiable persons will be considered processing covered by the data protection legislation.

2.3.1 Special categories of information

The processing may include specific categories of personal data pursuant to Article 9 of GDPR, if such data is covered by the report.

2.4 Processing activities

- Receive and screen reporting
- Assert impartiality
- Assess report
- Possible report to authorities
- Feedback to the whistleblower

2.5 Where does the processing take place?

The processing takes place on the premises of IATS.

The processing takes place in operational centres located in the EU.

2.6 Data processors

The IATS internal IT systems and whistleblower processors which are located in the EU.

2.7 Recipients of personal data (independent data controllers)

2.7.1 Authorities

If the inquiry gives rise to a report to an authority, the authority to which the report is made depends on the specific inquiry.

2.7.2 Transfer to 3rd countries and international organisations

Data is not transferred to countries outside the EU, nor to international organisations.

2.8 Erasure

The storage period depends on the specific case and what measures the case gives rise to. The information is erased as soon as it is no longer relevant in relation to documentation requirements vis-à-vis authorities, possible employment law disputes, etc.

Information covered by an unfounded report will be erased within 90 days of the final assessment.

2.9 Security measures

An access and user management system has been established for the IT system that the data processor uses for the whistleblower scheme, and the system also features encryption and ensures anonymity.

With regard to IATS's internal handling of information covered by a report, an access and user management system has also been established to ensure that only selected key employees have access to the information.