Privacy Policy pursuant to Article 13 of Regulation (EU) 2016/679 ("GDPR") on processing the personal data of individuals reporting misconduct

This Privacy Policy, provided in compliance with the Italian and European legislation on the protection of personal data ('Privacy Notice'), provides information on the processing of personal data carried out in the context of the receipt and management of reports of misconduct (the "Report" or the "Reports"), as required by the applicable regulations on *whistleblowing* (the "Whistleblowing Policy").

For further information on the categories of violations that can be reported on the reporting channels enabled within the ENAV Group, as well as on the methods for managing the Whistleblowing Reports received, please refer to the *Whistleblowing* regulation which, together with this notice, can be found on the *Whistleblowing* portal of the ENAV Group.

Joint data controllers

For the purposes concerning the receipt and management of the Whistleblowing Reports, in compliance with the applicable Privacy Regulations, the personal data of the Interested Parties (as defined below) are processed by the following companies belonging to the ENAV Group (the "Joint Controllers"):

ENAV S.p.A. with registered office in Via Salaria 716, Rome

D-flight S.p.A. with registered office in Via Salaria 716, Rome

IDS Air Nav with registered office in Via del Casale Cavallari 200, Rome

Techno Sky S.r.l. with registered office in Via del Casale Cavallari 200, Rome

The Joint controllers have signed an agreement regulating their responsibilities for processing personal data, as required by Article 26 of GDPR, the essential elements of which, referring to the processes related to Whistleblowing, are set out below:

- the joint-ownership agreement between the Joint Controllers will have the duration necessary to enable the proper management of the Whistleblowing Reports. Following the termination of this agreement, the Joint Controllers will retain and continue to process personal data for which they have or should have independent ownership by law, contract or established practice;
- the Joint Controllers shall process personal data only if such processing is based on an appropriate legal basis, cooperating and providing assistance to each other in proceedings initiated by or before the Data Protection Authority, and exchanging any information useful and necessary for the management of relations with that authority;
- the Joint Controllers shall jointly ensure the proper fulfilment of the obligations under the GDPR and the Privacy Legislation, including the obligations to adopt appropriate security measures applicable to the processing of personal data, to carry out an impact assessment, in accordance with and for the purposes of Article 35 of the GDPR where it is necessary for processing of personal data that is likely to involve a high risk for the rights and freedoms of data subjects, the obligations to provide adequate safeguards for any transfer of personal data to countries outside the European Economic Area, the obligation to deal promptly with any personal data breach occurrence (so-called *data breach*), etc.;
- the Joint Controllers will appoint the individuals authorized to process personal data, and the individuals responsible for processing personal data, in accordance with Articles 29 and 28 of the GDPR respectively;

In cooperation and coordination with each other, the Joint Controllers shall ensure the full exercise of the rights of the Interested Parties.

Accordingly, it should be noted that ENAV S.p.A. has appointed a Group Data Protection Officer, also referred to as *Data Protection Officer* ("DPO"), whose contact details are as follows:

- telephone: (+39) 0681661;
- e-mail: dpo@enav.it;
- certified email address: dpo.gruppoenav@pec.enav.it.

Please consider the DPO of ENAV S.p.A. as the point of contact for the Interested Parties at all the Joint Controllers.

Types of personal data processed and categories of data subjects

As part of the acquisition and subsequent management of Whistleblowing Reports, each Joint Controller, with the support of the Group functions, may process the following categories of personal data:

(i) contact details (e.g. telephone number, email address) and identification details (e.g. name and surname, identity documents) of the Data Subjects;

(ii) data relating to the office and/or role and/or work or professional duties performed by the Data Subjects;

(iii) the Whistleblowing Report and any other information provided when the Report is submitted, and/or for the management of the Whistleblowing Report and the related procedure;

(iv) data emerging from the investigations carried out for the verification of the Whistleblowing Report.

Where necessary, each Joint Controller will ensure that the processing of personal data belonging to special categories, as defined in Article 9 of the GDPR (*e.g.*, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or genetic data, biometric data, etc.), and/or judicial data, as defined in Article 10 of the GDPR, will be carried out in accordance with the Privacy Regulations.

The personal data processed by each Joint Controller belongs to the following categories of data subjects (hereinafter referred to as "**Data Subjects**"):

(i) natural person who makes a Whistleblowing Report to the competent judicial, administrative or accounting authority (including independent agencies such as ANAC) ("the Authority") and/or public disclosure (the "Whistleblower");

(ii) natural person named in the Whistleblowing, in the complaint to the competent authority and/or in the public disclosure, to whom the breach is attributed and/or who is implicated in the breach (the "Reported Party");

(iii) all natural persons whose personal data are processed in the context of a Whistleblowing Report or its handling in accordance with the applicable *whistleblowing* legislation, including, where applicable, natural persons who work and/or have worked for a Joint Controller (e.g. persons with administrative, management and/or supervisory functions; employees in any capacity and former employees; job applicants; trainees and probationary workers; shareholders; consultants and/or professionals; employees of contractors and service providers; solicitors or agents; etc.).

In addition to the above, the following categories of Data Subjects may also be recipients of the processing activities carried out by each Joint Controller, in the context of the receipt and/or management of the Whistleblowing Report:

(i) "facilitators", i.e. persons working in the same work environment as the Whistleblower;

(ii) persons linked to the Whistleblower or to the person making a complaint to the Authority and/or making a public disclosure, by a stable emotional or kinship link up to the fourth

degree and working in the same context; and

(iii) work colleagues of the Whistleblower and/or of the person who has made a complaint to the Authority and/or made a public disclosure, who work in the same work environment as the Whistleblower and who have a habitual and current relationship with that person.

Purpose and legal basis of processing

Each Joint Controller will process the personal data of the Data Subjects for the following purposes:

(i) fulfilment of regulatory obligations and pursuit of the relevant public interest related to the *Whistleblowing* Regulation;

(ii) management and assessment of the Whistleblowing Report transmitted with reference to the *Legislative Decree. n. 24/2023*, while respecting the right to confidentiality of the identity of the Whistleblower and the persons associated with him/her. Due to the provisions of the above-mentioned Legislative Decree, in the event that the report leads to the establishment of disciplinary proceedings against the person responsible for the illicit conduct, the whistleblower's identity will never be revealed. If revealing the identity is necessary for the accused's defense, the whistleblower will be asked for explicit consent.

(iii) Joint Controllers' internal control and monitoring of business risks, as well as for the optimization and streamlining of internal business and administrative processes, based on the legitimate interest of the Joint Controllers themselves;

(iv) establishment, exercise or defense of a right and/or legitimate interest of the Joint Controllers or third parties in any competent forum;

(v) fulfilment of any requests by the competent authorities (e.g. ANAC, judicial authorities, judicial police).

The legal bases of the above-mentioned processing are represented by the fulfillment of legal obligations, the consent and the pursuit of the legitimate interests of the Joint Controllers, pursuant to article 6, paragraph 1, letters a), c) and f) of the GDPR.

The Joint Controllers inform that data belonging to special categories, as defined pursuant to Article 9 of the GDPR, may be processed for reasons of relevant public interest, pursuant to and within the limits of Article 9, letters b), f) and/or g) of the GDPR and within the limits of the "Privacy Code", namely for the purpose of combating the offences identified by the *Whistleblowing* Regulations, as well as for the protection of the Whistleblower and other persons treated as such. In certain cases, related to the management of the Whistleblowing Reports, special data may also be processed in order to (i) fulfil the obligations and exercise the rights of Joint Controllers in the field of labour law, protection and/or social security or (ii) exercise or defend a right, including in court.

Within the limits of the above-mentioned relevant public interest, as described and circumscribed by applicable laws, judicial data may also be processed pursuant to Article 10 GDPR.

Communication and distribution of personal data

Authorized personnel will process collected personal data, they will be appointed in advance pursuant to Article 29 of the GDPR, and will not be distributed.

Please refer to the *Whistleblowing* regulation for more information on the personnel in charge and the ENAV Group bodies authorised to receive and handle Whistleblowing Reports.

Personal data may also be processed by parties external to the Joint Controllers where expressly appointed, as data processors pursuant to Article 28 of the GDPR (e.g. *auditing*/review companies, system and application suppliers, companies contractually linked to the Joint Controllers).

This is without prejudice, in any case, to the communication of the requested data, in accordance with the law, to the entities concerned, competent authorities (e.g. the National Anti-Corruption Authority), security bodies or other public entities for the purposes of public interest within their competence, which will process the data as autonomous data controllers.

Personal data provided and/or collected will be transferred to third country authorities, companies and/or international organisations located outside the territories of the European Union, only in cases where there is a legal obligation on the Joint Controllers, or in compliance with the appropriate guarantees provided for in Article 46 GDPR (e.g. standard contractual clauses).

Personal data retention period

The data will be retained for up to 5 years from the final communication of the outcome of the Whistleblowing Reporting procedure and will be processed for a period of time not exceeding that which is indispensable to achieve the purposes for which they are collected; after that, they will be retained in order to comply with legal obligations and/or to assert and/or defend the rights and/or legitimate interests of the Joint Controllers or of third parties, including in the event of claims, litigation or pre-litigation. If the report is not followed up after the preliminary acceptance and admissibility, the retention period will be reduced to a maximum of 60 days.

Methods used to process personal data

The processing operations of the personal data of the Data Subjects are carried out on paper or with the aid of electronic or automated means suitable to guarantee the necessary security in relation to the nature of the data processed. In particular, the Joint Controllers guarantee that the processing of personal data is carried out with respect for the fundamental rights and freedoms, as well as the dignity of the Data Subjects with particular reference to confidentiality and data security. All information processed for the purposes of this document is also subject to compliance with the ENAV Group's *Security Management System*.

Digital data are stored in secure servers located in access-controlled areas with restricted access and specific technical and organisational security measures (*i.e.* encryption) to protect the contents of the Reports, both in transit and in archives. Should the report be sent by paper means, it and any accompanying documentation (including identity documents) will be stored in a secure location at the Internal Audit offices.

Rights of data subjects

The Data Subjects have the right to obtain access to the following information: the purposes of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data have been or will be disclosed (including recipients in third countries or international organisations), the expected storage period of the personal data or, if this is not possible, the criteria used to determine this period, the origin of the personal data, the existence of a profiling process and information on the logic used.

In addition, they have the right to:

- obtain the rectification of inaccurate personal data;
- obtain the integration of incomplete personal data;
- obtain the restriction of the processing of personal data (in which case, the data are processed only with the express consent of the data subjects, except for the necessary storage of the data);
- object to their processing;
- obtain removal ("right to be forgotten").

As per the Privacy Code and ENAV Group’s data protection policies, the Joint Controllers inform the Interested Parties that the rights provided for in Articles 15 to 22 of the GDPR may be subject

to limitations (e.g. delay) and/or preclusions (non-acceptance by the Joint Controllers) if their exercise may result in an actual and concrete prejudice to the protection of the confidentiality of the Whistleblower and its subjects, and/or to the carrying out of investigations or to the exercise of a right in court by the Joint Controllers.

This is without prejudice to the right of the Reported Party to exercise his or her rights by requesting the intervention of the Data Protection Authority, in the manner provided for in the Privacy Code.

To exercise the above-mentioned rights, the Data Subjects may contact the DPO of the ENAV Group, using the contact details provided in this Privacy Policy.

This Privacy Policy is updated to October 2024