ASTAIR Requirement No. 2 POPD

Deliverable ID:	**D7.4**
Project acronym:	**ASTAIR**
Grant:	**101114684**
Call:	**HORIZON-SESAR-2022-DES-ER-01**
Topic:	**HORIZON-SESAR-2022-DES-ER-01-WA1-1**
Consortium coordinator:	**Ecole Nationale de L'Aviation Civile (ENAC)**
Edition date:	**09 February 2024**
Edition:	**01.01**
Status:	**Official**
Classification:	**PU**

Abstract

ASTAIR project hereby acknowledges that ethics is given the highest priority in EU funded research and that activities carried out under Horizon Europe must comply with ethical principles and relevant national, EU and international legislation, such as the Charter of Fundamental Rights of the European union and the European Convention on Human Rights.

ASTAIR project hereby also acknowledges that pursuant to the Grant Agreement the beneficiaries must carry out the action in compliance with:

- Ethical principles (including the highest standards of research integrity as set out, for instance, in the European Code of Conduct for Research Integrity and including, in particular, avoiding fabrication, falsification, plagiarism or another research misconduct),
- Applicable international, EU and national law.

ASTAIR plans to organize web surveys, interviews, workshop events and validation activities.

The ethic requirement that has been identified for ASTAIR is the Protection of Personal Data (POPD).

Authoring & approval

Author(s) of the document

Organisation name	Date
ENAC	21 November 2023

Reviewed by

Organisation name	Date
TU Delft	24 Nov. 2023
ADP	27 Nov.2023
Eurocontrol	27 Nov.2023
Deep Blue	27 Nov.2023

Approved for submission to the SESAR 3 JU by[1]

Organisation name	Date
TU Delft	24 Nov. 2023
ADP	28 Nov 2023
Eurocontrol	29 Nov. 2023
Deep Blue	29 Nov. 2023
ENAC	29 Nov. 2023

Rejected by[2]

Organisation name	Date

Document history

Edition	Date	Status	Company Author	Justification
00.01	21/11/2023	Draft	ENAC	1st version
01.00	29 Nov. 2023	Release	ENAC	Corrected after internal reviews

[1] Representatives of all the beneficiaries involved in the project

[2] Representatives of the beneficiaries involved in the project

ASTAIR

AUTO-STEER TAXI AT AIRPORT

ASTAIR

This document is part of a project that has received funding from the SESAR 3 Joint Undertaking under grant agreement No 101114684 under European Union's Horizon Europe research and innovation programme.

Table of contents

1 Introduction

ASTAIR goal is to design a seamless partnership between Human and Artificial Intelligence (AI) to manage and perform engine-off and conventional taxiing operations on all the airport surfaces (including aircraft and towing vehicles steering from the gates to the runways at major European airports). Increasing the level of automation overlooking all ground movements will help increase the general predictability of airport turnaround operations and cope with the additional complexity induced by engine-off taxiing techniques.

This document describes the compliance of project ASTAIR with the ethics requirements POPD – Requirement No.2 (Processing of Personal Data). In particular, the following points will be addressed:

- ENAC Data Protection Officer
- Data minimization principle

Data storage and protection

1.1 Applicable Reference material

Unless otherwise stated, the execution of the project **will be fully compliant** with the latest version of the S2020 Project Handbook available in STELLAR Program Library.

[1] ASTAIR Grant Agreement Description of Action - GA-101114684-ASTAIR

[2] Regulation (EU) 2016/679 (General Data Protection Regulation)

[3] European Data Protection Board **Guidelines on consent under Regulation 2016/679, WP259 rev.01** superseded by **Guidelines 05/2020 on consent under Regulation 2016/679**

[4] Ethics and data protection: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

2 Data Protection Policy

POPD 'Protection of Personal Data' is involved in any operation (or set of operations) performed on personal data either manually or automatically, from collection, storage, usage to destruction.

ASTAIR project foresees a number of activities and resources which could potentially require the processing of personal data:

- Website
- Web surveys
- Workshops
- Validation activities

2.1 Identification of the Controller

ENAC as the ASTAIR project coordinator will act as the controller of all the personal data collected by the project. The Controller is responsible for ensuring GDPR compliance and controls the procedures and purpose of data usage in collaboration with the partners' Data Protection Officer.

2.2 Data Protection Officers

ASTAIR partners have designated a Data Protection Officer (DPO) to comply with all the data protection requirements in accordance with all the applicable data protection regulations. Each partner can manage the data it has collected, with the agreement and under the supervision of the Controller. However, ENAC can also provide an access protected storage space on its own server for data safeguard (see 2.4).

Contact information for the DPO of each partner are the following:

- ENAC: Estelle Corbel, dpo@enac.fr
- TU Delft: Heather Andrews, H.E.AndrewsMancilla@tudelft.nl
- Deep Blue: Vera Ferraiuolo, dataprotectionofficer@dblue.it
- ADP: informatique-libertes@adp.fr
- Eurocontrol: data-protection-officer@eurocontrol.int

These contact information will be provided prominently in any activity or resource that involves personal data processing, depending on the data collection responsible.

2.3 Relevance of collected data

The purpose for the processing of each category of personal data will be specifically indicated further on for every ASTAIR activity, specially focusing on communication and dissemination activities. The

ASTAIR Consortium will process Personal data on a lawful basis, as provided in Articles 6 and 9 of the GDPR[2].

WEBSITE

ASTAIR website and social media will sustain communication activities allowing ASTAIR to target a larger audience. On ASTAIR website will be created a dedicated section with cookie policy to inform users about how their data will be used. Any data required by the website serves the correct functioning of the service. Users' data will never be sold or exchanged with anyone external to the project consortium. The project will collect only data to monitor and analyse web traffic, and to keep track of user behaviours. Using only aggregated data will guarantee user anonymity. Further, once ASTAIR will end all the sensible data will be deleted.

SURVEYS

Web surveys will typically circulate in digital form and will be collected by email or through dedicated platforms (for example: Google Forms or similar).

The collection will be performed by Deep Blue.

Participants' opinions, experiences, comments, ideas, and feedback will possibly be collected through questionnaires designed by the ASTAIR consortium.

The topics of the questionnaires will focus the development of engine-off taxiing techniques and on the feasibility and expected impact on the Aviation operations of selected operational improvements proposed by the consortium.

WORKSHOP

Participants to workshops are either invited personally or voluntarily register. The following personal data are needed and recorded by ASTAIR Partners: First name and Last name, Organisation, Email address. Workshops will be organized by all the ASTAIR partners.

More information for personal identification could be required to access the premises of the workshop, as the workshop may be hosted by international organizations or private companies.

The personal data will be collected and communicated to the host organization / company but not stored by ASTAIR Partners: First name, Last name, Nationality. Information about food allergies could be necessary for those workshop that include meals.

During workshop activities, participants may work in work sessions and provide personal opinions, experiences, comments, on safety research released topics. These data will be anonymised or pseudonymised

Only aggregated results will be recorded and shared by ASTAIR Partners. Depending on the workshop topic, results may be shared with workshop participants, with the ASTAIR consortium, with the SJU Project Officer, or made publicly available via the ASTAIR website.

The workshop may be video recorded, and photos may be taken for dissemination and communication purposes. Photos and videos will typically be edited and made publicly available via the ASTAIR website and newsletter. No spoken statement will be included in these videos, but only images of participants.

Workshop participants might be contacted for future workshops or dissemination events or the newsletter distributed to them. For these purposes, the ASTAIR will retain only their first name and last name, organization, email.

VALIDATION ACTIVITIES

Participants to validation activities are either selected due to the contribution they can offer to ASTAIR research. The following personal data are needed and recorded by ASTAIR Partners: First name and Last name, Organisation, Email address. All ASTAIR partners will participate to the validation of the project findings. During the validation and all the related to activities, the Consortium will act in compliance with the GDPR.

2.4 Artificial Intelligence

Although ASTAIR concept is built upon an artificial intelligence module, this module is developed as a Multi-Agent System (MAS) and do not rely on machine learning.

Machine learning is a subset of artificial intelligence that focuses on developing algorithms allowing computers to learn patterns from data without explicit programming. It typically involves training a model on a large dataset to make predictions or decisions. On the other hand, multi-agent systems involve multiple autonomous entities, or agents, interacting with each other to achieve individual or collective goals. While machine learning relies heavily on data to train models for specific tasks, multi-agent systems emphasize decentralized decision-making and coordination among independent agents, on ASTAIR without a central dataset-driven learning approach.

2.5 Measures to safeguard personal data

According to Article 24 of the GDPR, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation itself.

The ASTAIR Consortium is committed to ensuring the effective protection of Personal data of all participants to its activities.

SECURITY MEASURES

The ASTAIR Consortium is committed to implement appropriate technical and organisational measures to guarantee in an effective manner the necessary safeguards for the processing of personal data. Article 32 of the GDPR recommends pseudonymisation and encryption of personal data as security measures which should ensure a level of security appropriate to the risk of processing. Pseudonymisation is “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person” (Art. 4 par. 1 n. 5).

Pseudonymisation and other security measures will be implemented in full compliance with the most recent rules, opinions and guidelines from European and national competent Authorities.

No data, which is not strictly necessary to accomplish the current study, will be collected; data minimization policy will be adopted at any level of the study and will be supervised by the ethical

committee of the study; any shadow (ancillary) personal data obtained in the course of the observation will be immediately cancelled.

Data presented in publications or to employers will use aggregated data only, in which individuals cannot be identified. Pictures, videos and audios will be recorded only after the signature of a detailed Information Sheet and Consent Form. Also, for videos and images, participants' faces will be covered with a masking filter to prevent identification. For audio files, no name of participant, facilities, and companies will appear on audio files. Audio filters that distort voices will also be applied. The audios and videos will be not be used for any different purposes, nor disclosed to any third party and will be destroyed 2 years after the end of the project.

DATA STORAGE

Data will consist of digital or/and paper data. Digital data will be stored on hard disks disconnected from the network, which will be stored in secured drawers; and/or on secured servers, with defined protocol that limit access to authorized personnel.

Latest encryption techniques will be applied to all digital data.

Paper data will be stored in secured drawers with access limited to authorized personnel.

ENAC provides different storage spaces, with a protected access, depending on the need:

- Redmine: ENAC hosts a private instance of a Redmine server[3] (https://git.recherche.enac.fr) which provides a wiki and a document storage space for general project related information
- Git: ENAC's Redmine instance is coupled with a Git server[4] for configuration management
- Private cloud: if a larger space is needed for collected data, ENAC can also provides storage on its own instance of NextCloud[5](https://cloud.recherche.enac.fr/).

DATA RETENTION

Project documentation, including technical documents describing the results of research activities, will be archived after the end of the project in password-protected servers.

DATA DESTRUCTION

Data will be destroyed two years past the termination of the project. Paper data will be physically destroyed. Digital data will be overwritten to ensure that they are effectively scrambled and remain inaccessible.

DATA BREACHES

In the case of a personal data breach, the controller will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with GDPR rules, unless the personal data breach is unlikely to

[3] https://www.redmine.org/

[4] https://git-scm.com/

[5] https://nextcloud.com/

result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The controller prepared an internal policy to manage the event of a data breach in accordance to the GDPR. Every person affiliated to one of the ASTAIR partners has to report a suspected data breach to the following email address without undue delay mathieu.cousy@enac.fr.

2.6 Informed consent procedures

The processing of Personal data will be based on **Consent** (for common Personal data) and **Explicit Consent** (for special categories of Personal data).

Consent of the data subject has to be freely given, specific and informed. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

As requested in Article 7 of the GDPR, the ASTAIR Consortium will be able to demonstrate that all data subjects have consented to processing of their Personal data. Explicit consent will be obtained before processing special categories of personal data, such as food allergies and personal opinions.

According to the WP29 Guidelines[6] on Consent, consent of the data subject means any:

- freely given,
- specific,
- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The ASTAIR Consortium will ensure the so called “granularity” of consent: “A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes” (Guidelines, p. 3.1.3 [3]).

Prior to obtaining their consent, participants to ASTAIR activities will always be provided with information listed in Article 13 of GDPR, and with any communication under Articles 15 to 22 and 34 of GDPR relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

In all ASTAIR activities no Personal data will be processed without Informed, specific, explicit consent of the data subjects. The main user groups targeted are professionals working in the aviation domain

[6] https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en

(e.g. airspace users, air navigation service providers, airport operators, staff associations and their members, manufacturing associations and their members, institutional decision-makers, media, researchers, etc.). Engaged stakeholders will have the competence to understand written and oral informed consent information.

ASTAIR research will NOT include children, adults unable to give informed consent, nor vulnerable individuals/groups.