DATA PROTECTION ADMINISTRATIVE ARRANGEMENT

BETWEEN

THE SINGLE EUROPEAN SKY ATM RESEARCH 3 JOINT UNDERTAKING

AND

EUROCONTROL

Ref. S3JU [redacted]

The **SINGLE EUROPEAN SKY ATM RESEARCH 3 JOINT UNDERTAKING**,

Hereinafter referred to as "SESAR 3 JU", a Joint Undertaking within the meaning of Article 187 of the Treaty on the Functioning of the European Union and set up by Council Regulation (EC) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe[1],

Having its seat located at 100 Avenue de Cortenbergh,
1000-Brussels
Belgium

Represented for signing this DPAA by [redacted], its Executive Director,

OF THE ONE PART,

AND

EUROCONTROL[2],

Hereinafter referred to as "EUROCONTROL", established by the EUROCONTROL International Convention relating to Co-operation for the Safety of Air Navigation as amended at Brussels in 1981 (the "Convention"),

Having its headquarters located at Rue de la Fusée, 96
B-1130 Brussels,
Belgium

Represented for signing this DPAA by [redacted], the Director General,

OF THE OTHER PART,

Hereinafter referred to individually as a "Party" and collectively the "Parties".

[1] Council Regulation (EU)2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014

[2] The European Organisation for the Safety of Air Navigation

RECITALS

HAVING REGARD to Governing Board ref. [redacted] adopting the SESAR 3 JU – EUROCONTROL Administrative Agreement under Articles 157 and 158 of the SBA, including any future amendment;

HAVING REGARD to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance);

Having regard to the EUROCONTROL Regulation on Personal Data Protection approved by the Permanent Commission through Measure 06/129 of 28.12.2006 and its Implementing Rules applicable to EUROCONTROL;

Whereas Article 41(1) of Regulation (EU) 2018/1725 establishes that any Union body shall inform the European Data Protection Supervisor when drawing up administrative measures and internal rules relating to the processing of personal data by a Union institution or body, whether alone or jointly with others;

Whereas Article 48(3)(b) of Regulation (EU) 2018/1725 establishes that in the absence of an adequacy decision, a controller may transfer personal data to an international organisation by, inter alia, provisions to be inserted into an administrative arrangement between public authorities or bodies which include enforceable and effective Data Subject rights, subject to the authorisation from the European Data Protection Supervisor;

Whereas SESAR 3 JU informed and consulted the European Data Protection Supervisor under Articles 41 and 48(3)(b) of Regulation (EU) 2018/1725;

Whereas, on the basis of Article 48(3)(b) of Regulation (EU)2018/1725, the European Data Protection Supervisor authorised the safeguards developed under this DPAA under decision… dated…;

In consideration of the above, the Parties have agreed as follows:

ARTICLES

1 DEFINITIONS

In this Data Protection Administrative Arrangement (DPAA), unless the context requires otherwise:

- the singular includes the plural and vice versa;
- any phrase introduced by the words "including", "includes", "in particular", "for example" or similar, shall be construed as illustrative and without limitation to the generality of the related general words.

The headings in this DPAA are for ease of reference only and shall not affect its interpretation.

References to Articles and Annexes are, unless otherwise stated, references to the Articles and Annexes to this DPAA.

If there is any conflict within or between the Administrative Agreement and the Articles and any Annex of the DPAA, the conflict shall be resolved in accordance with the following order of precedence:

- The Council Regulation establishing the Single European Sky ATM Research 3 Joint Undertaking (SESAR 3 JU) under Horizon Europe (the "Single Basic Act" or " SBA");
- Articles of the DPAA;
- Annexes of the DPAA; and
- Any other document referred to in the DPAA;
- Articles of the Administrative Agreement.

For the purpose of the DPAA, the following definitions shall apply:

Adequacy Decision	A decision where the European Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680 that a third country, a territory or one or more specified sectors within that third country, or an international organisation ensure an adequate level of data protection
Administrative Agreement	Administrative Agreement art. 157 and 158 of Council Regulation (EU) 2021/2085 of 19 November 2021 between the Single European Sky ATM Research 3 Joint Undertaking and EUROCONTROL ref.: S3JU [redacted], ECTL Ref:
Applicable Data Protection Legislation	Any data protection regulation that may apply to each Party in the context of the DPAA, including, where applicable, Regulation (EU) 2018/1725 applicable to the SESAR 3 JU, and the EUROCONTROL Regulation on Personal Data Protection, Permanent Commission Measure 06/129 of 28.12.2006, its Implementing Rules, Office Notice 25/17 of 25 October 2017, applicable to EUROCONTROL
CJEU	Court of Justice of the European Union

Controller	The natural or legal person, Union institution or body, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed under this DPAA.
Data Protection Register	The record of processing activities that each Party shall maintain under its responsibility as per the Applicable Data Protection Legislation.
Data Subject	An identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number or to one or more factors specific to his physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.
Data Protection Administrative Arrangement or "DPAA"	The agreement between SESAR 3 JU and EUROCONTROL in accordance with article 48(3)(b) of Regulation (EU) 2018/1725, which subject to the authorisation of the EDPS will govern any transfer of personal data between the Parties, as well as any onward transfers of that data.
EEA	European Economic Area
European Data Protection Supervisor or "EDPS"	The supervisory authority concerning the processing of personal data by SESAR 3 JU, established under article 52 of Regulation (EU) 2018/1725.
Onward transfer	Further transfer of personal data by the Receiving Party, to an entity who is not a Party to the DPAA. This includes further transfers to entities located in a Member State of the European Union or a country that is part of the European Economic Area, in a country or an international organisation that benefits from an adequacy decision adopted by the European Commission pursuant to Article 45 of Regulation (EU) 2016/679, as well as in other countries and international organisations not covered by the first part of this sentence.
Personal Data	Any information relating to an identified or identifiable natural person ("Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	A natural or legal person, public authority, agency or any other body, which process personal data on behalf of a Party (controller). Parties may engage a processor to provide goods or services that directly relate to the execution of the activities under the DPAA.
PMU or "Programme Management Unit"	Organisational Unit composed of around twenty (20) staff provided by EUROCONTROL, as described in Schedule 3, Appendix 2.1 of the Administrative Agreement
Receiving Party	The Party, which under this DPAA receives from the other Party the personal data mentioned in Annex I.
Recipient	A natural or legal person, public authority, agency or another body, which is not party to this DPAA.
Regulation (EU) 2018/1725 ('EUDPR')	Regulation (EU) 2018/1725 of the European Parliament and of the council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
Single Basic Act or "SBA"	Regulation, establishing the SESAR 3 Joint Undertaking, i.e. Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014.
Transfer	Disclosing by transmission or otherwise making personal data available from the Transferring Party to the Receiving Party, whereas the Receiving Party is an international organisation.
Transferring Party	The Party, which under this DPAA transfers the personal data mentioned in Annex I to the other Party.

2 SCOPE OF THIS ADMINISTRATIVE ARRANGEMENT

2.1 The DPAA sets the allocation of respective roles, responsibilities and practical arrangements for compliance of the Parties with their respective data protection obligations where they transfer the necessary Personal Data pursuant to the Applicable Data Protection Legislation.

2.2 The DPAA sets the appropriate safeguards required under Article 48 of Regulation (EU) 2018/1725, for the transfer of personal data between SESAR 3 JU and EUROCONTROL.

2.3 Personal data transferred between the Parties shall be processed in line with the Applicable Data Protection Legislation and the definitions and requirements set out in this DPAA.

3 PURPOSES AND SCOPE OF THE TRANSFER

3.1 The transfer of Personal Data is necessary to support the following purposes further detailed in Annex I:

a) Functioning of the Programme Management Unit as described in Appendix 2.1 of the Administrative Agreement;
b) Promotion, outreach and stakeholder relations as described in Appendix 2.2 of the Administrative Agreement;
c) Provision of specialist support and advice as described in Appendix 2.3 of the Administrative Agreement;
d) Provision of Information and Communication Technologies support services to the SESAR 3 JU as described in Appendix 3.2 of the Administrative Agreement;
e) Provision of logistics and infrastructure support, as described in Appendix 3.1 of the Administrative Agreement.

3.2 Transferred Personal Data shall not be used for any purpose other than those expressly mentioned in this article. The Parties shall process personal data for further purposes, only when they are compatible with the original purpose and only after notifying each other, giving the other Party the opportunity to object and updating Annex I. Further purposes compatible with the original purposes are archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

4 DATA SUBJECTS

The Data Subjects whose personal data are transferred according to the DPAA are identified in Annex I.

5 PERSONAL DATA

5.1 The Personal Data transferred between SESAR 3 JU and EUROCONTROL are identified in Annex I.

5.2 Personal Data that are not required in the framework of the DPAA between the SESAR 3JU and EUROCONTROL shall be deleted or returned immediately to the Transferring Party.

5.3 The Parties shall ensure that Personal Data transferred under the DPAA is accurate, up to date and only accessible by the Receiving Party's staff on a need-to-know basis.

5.4 If one of the Parties becomes aware that inaccurate or out of date Personal Data has been transferred or is being processed, it must notify the other Party without delay.

5.5 Where it is confirmed that Personal Data transferred is inaccurate, each Party shall take every reasonable step to rectify or erase such Personal Data.

6 ONWARD TRANSFERS

6.1. The Receiving Parties may onward transfer the personal data only when necessary and justified for the fulfilment of the tasks described in Annex 1 which are recognised in the legal framework applicable to SESAR 3 JU.

6.2 In addition, the Receiving Parties may only onward transfer the personal data to a third party located outside of the EEA or to an international organisation if:

- the country where the third party is located or the international organisation benefits from an Adequacy Decision adopted by the European Commission pursuant to Article 45 of Regulation (EU) 2016/679 (adequacy decision) that covers the onward transfer; or
- the third party is listed in Annex III and enters into a binding commitment to ensure the same level of data protection as provided by this DPAA, including with respect to the rights of data subjects; or
- the Transferring Party expressly authorises an onward transfer to a third party not listed in Annex III that enters into a binding commitment to ensure the same level of data protection as provided by this DPAA, including with respect to the rights of data subjects. Before requesting the authorisation, the Receiving Party shall provide the information required under Annex III to the Transferring Party in support to its request for authorisation. The Transferring Party shall keep a record of such notifications and provide its supervisory authority with this information upon request.

6.3 Where none of the conditions of 6.2 apply and if the requirements of 6.1 are met , the Receiving Party may only onward transfer personal data, in individual and exceptional cases, provided that:

a. the Receiving Party has obtained the explicit consent of the data subject for the onward transfer, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer in terms of applicable data protection safeguards; or
b. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person; or
c. the onward transfer is necessary for the establishment, exercise or defence of legal claims; or
d. the third party commits to process the data only for the specific purpose(s) for which it is onward transferred and to immediately delete it once the processing is no longer necessary for that purpose.

The Receiving Party shall notify the Transferring Party of such transfers before they take place by providing the information required under Annex 3, or, if that is not possible, immediately thereafter. The Receiving Party shall keep a record of such notifications and provide its supervisory authority with this information upon request.

7 PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

In order to guarantee compliance with applicable data protection rules, each of the Parties shall comply with the general principles of data protection as laid down in the Applicable Data Protection Legislation. In particular, Parties shall process personal data in accordance with the principles of:

a) Lawfulness, fairness and transparency, meaning that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject

b) Purpose limitation, meaning that personal data is collected for specified, explicit and legitimate purposes in the framework set out in Article 3 above and not further processed in a way incompatible with those purposes;
c) Data minimisation, meaning that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accuracy, meaning that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate or incomplete personal data are erased or rectified without delay;
e) Storage limitation, meaning that personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed as per article 11 below;
f) Integrity and confidentiality, meaning that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
g) Accountability, meaning that the Parties shall be responsible for, and be able to demonstrate compliance with the principles listed above (subparagraph (a) to (f)).

8 TRANSPARENCY AND MODALITIES

8.1 Transparent information and communication

8.1.1 The Parties shall include a general information notice on their websites with, information on how and why they may transfer personal data under the DPAA, the tool used for the transfer, the entities to which such data may be transferred, the rights available to Data Subjects and applicable restrictions, available redress mechanisms and contact details for submitting a dispute or claim.

8.1.2 The Parties shall publish the DPAA on their website and make the DPAA available to Data Subjects upon their request free of charge. To the extent necessary to protect confidential information, including personal data, the Parties may redact parts of the DPAA prior to sharing a copy, but shall provide a meaningful summary if the data subject would otherwise not be able to understand its content or exercise his/her rights.

8.2 Modalities for the exercise of Data Subjects' rights and handling of Data Subject requests

8.2.1 The Data Subjects may exercise their rights under the Applicable Data Protection Legislation in respect of and against the Party concerned by the Applicable Data Protection Legislation. In particular, Data Subjects may exercise the following rights:

- **Right of information**, meaning the Data Subjects' rights to receive information on the processing of personal data relating to him or her in a concise, transparent, intelligible and easily accessible form;
- **Right of access**, meaning confirmation as to whether or not personal data concerning them are being processed, and where that is the case, to access the personal data and to obtain specific information concerning the processing, including the purpose of the processing, the categories of personal data concerned, the Recipients to whom personal data is disclosed, the envisaged storage period and redress possibilities;

- **Right to rectification**, meaning the right to have the Data Subject's inaccurate personal data corrected or completed without undue delay;
- **Right to erasure**, meaning the right to have their personal data erased where the personal data are no longer necessary for the purposes for which they were collected or processed, or the Data Subject withdraws consent or objects to the processing or where the data have been unlawfully collected or processed or they need to be erased for compliance with a legal obligation to which a Party is subject;
- **Right to restriction of processing**, meaning the Data Subjects' right to restrict the processing of their personal data where the personal data are inaccurate, where the processing is unlawful, where the Parties no longer need the personal data for the purposes for which they were collected or where the personal data cannot be deleted;
- **Right to data portability** meaning the Data Subjects' right to receive the personal data concerning them, which they have provided to a Party, in a structured, commonly used and machine-readable format and transmit those data to another controller. This right shall be applicable if processing is based on consent or for the execution of a contract and the processing is carried out by automated means;
- **Right to object**, meaning the Data Subjects' right to object on ground relating to his or her particular situation at any time to processing of personal data concerning him or her by a Party, except in cases where there are compelling legitimate grounds for the processing that override the grounds put forward by the Data Subject or for the establishment, exercise or defence of legal claims;
- **Right not to be subject to automated decision-making, including profiling**, meaning the Data Subjects' right not to be subject to legal decisions concerning them based solely on automated processing, unless the decision is necessary to enter into a contract, authorised by Union Law or based on the Data Subjects' consent.

8.2.2 The Parties shall cooperate and provide each other with reasonable assistance in addressing any Data Subject request concerning the exercise of Data Subject rights, and with respect to security, Data Breach notifications and impact assessments in compliance with the Applicable Data Protection Legislation. The Parties shall render all the assistance required and provide information necessary for the other Party to comply with its obligations with its supervisory authority.

8.2.3 Data Subjects may exercise the rights listed above before any of the Parties. In addressing Data Subjects' requests, the Parties shall inform each other about the receipt of any Data Subject request relating to Personal Data transferred under the DPAA and consult each other before disclosure of Personal Data.

8.2.4 In particular, when the request does not fall under its responsibility, the Party shall promptly, and at the latest within five (5) calendar days, forward the request to the responsible Party.

8.2.5 The SESAR 3 JU may apply possible restrictions to Data Subjects rights, as laid down in Article 25 of Regulation (EU) 2018/1725 only if necessary to safeguard the rights of Data Subjects and/or the rights and freedom of others, under the conditions foreseen in the dedicated SESAR 3 JU Decision on Restrictions available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022Q0513(01)&from=EN.

8.2.6 Each Party, shall handle in a reasonable and timely manner without undue delay, and in any case within one month, extendable at maximum by two further months where necessary,

taking into account the complexity and number of the requests, a request from a Data Subject concerning the above rights.

The Parties shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

8.2.7 In case the Parties do not take action on the request of the Data Subject, without delay and at the latest within one month of receipt of the request, the Parties shall inform the Data Subject with the reasons for not taking action and on the possibility of lodging a complaint and of seeking a judicial remedy.

9 SECURITY OF PROCESSING

9.1 Annex II of the DPAA details technical and organisational measures, designed to:

a) Ensure and protect the security, integrity and confidentiality of the Personal Data transferred, respectively in line with the applicable Data Protection legislation and internal procedures;

b) Protect against any unauthorised or unlawful processing, loss, use, disclosure or acquisition of or access to any Personal Data in its possession;

9.2 The Parties shall cooperate as per the mechanisms agreed in Article 13 of this DPAA with a view to addressing any issues stemming from differences between their respective security policies.

10 SECURITY INCIDENTS AND DATA BREACHES

10.1 The Parties shall handle security incidents, including Data Breaches, in accordance with their internal procedures and Applicable Data Protection Legislation, in particular, they shall provide each other with swift and efficient assistance to facilitate the identification and handling of any security incident, including Data Breaches, linked to personal data transferred under the DPAA, in application of the Applicable Data Protection Legislation.

10.2 Accordingly, they shall notify each other without undue delay and at the latest within 48 hours upon becoming aware of the security incident/Data Breach about:

a) Actual risks to the confidentiality, integrity or availability of the transferred Personal Data and/or;

b) Security incidents that are linked to the transferred Personal Data to the extent that they present a risk to the other Party or the Data Subjects;

c) Breaches of the technical and/or organisational safeguards of the purposes covered by this DPAA to the extent that they present a risk to the other Party or the Data Subjects.

10.3 The notification of a Data Breach shall include a description of the likely consequences of the personal data breach, the assessment of the risk to the rights and freedoms of natural persons,

as well as any measures taken to address the personal data breach and to mitigate the risk to the rights and freedoms of natural persons.

10.4 The SESAR 3 JU shall notify any personal Data Breach to the EDPS within 72 hours from becoming aware of the personal Data Breach, in accordance with Article 34 of Regulation (EU) 2018/1725. EUROCONTROL shall render the SESAR 3 JU all the assistance required and provide information necessary for the SESAR 3 JU to comply with its obligation.

10.5 If the Data Breach is likely to result in a risk to the rights and freedoms of natural persons, the Party responsible for the Data Breach shall communicate that Data Breach to the Data Subjects concerned, in accordance to the Applicable Data Protection Legislation. The Party responsible shall inform the other Party of such communication.

10.6 The Party responsible for a Data Breach is either:

a) The Party responsible for the business process that is the source of the Data Breach by design (of processes, IT systems, workflows of data etc.);

Or

b) The Party responsible for the staff to whom the Data Breach can be attributed as a result of:
   1) Specific personal data processing operations outside the corporate workflows;
   2) Deviations from the corporate business processes, as documented and implemented;
   3) Misuse of the IT tools;
   4) Any other personal data processing operations not covered by the scope of this DPAA.

11 DATA RETENTION

11.1 Parties shall not retain or process Personal Data transferred under the DPAA longer than the duration specified under Annex I for each identified transfer.

11.2 In complement to article 3.2 when retention of personal data is required for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the Parties shall specify such retention period in Annex I in advance.

12 REMEDIES AND LIABILITY

12.1 The SESAR 3 JU is liable for non-compliance in line with Chapter VIII of Regulation (EU) 2018/1725. EUROCONTROL shall render the SESAR 3 JU all the assistance required and provide information necessary for the SESAR 3 JU to comply with its obligations.

12.2 Should a Data Subject believe that the SESAR 3 JU failed to comply with the appropriate safeguards set forth in the DPAA, he or she may lodge a complaint with the SESAR 3 JU Data Protection Officer.

If the Data Subject believes that the SESAR 3 JU did not resolve the complaint appropriately, he or she may lodge a complaint with the European Data Protection Supervisor for administrative redress and seek judicial remedy, including compensation for material and non-material damages, before the Court of Justice of the European Union.

12. 3 Should a Data Subject believe that EUROCONTROL failed to comply with the appropriate safeguards set forth in this DPAA, he or she may lodge a complaint with the EUROCONTROL Data Protection Officer.

12.4 During a transition period finishing by 31 December 2023, if the Data Subject believes that the complaint was not resolved appropriately by EUROCONTROL, he or she may seek administrative redress and remedies, including compensation for material and non-material damages, towards EUROCONTROL by arbitration by filing a claim before the International Court of Arbitration of the International Chamber of Commerce ("ICC") in accordance with the ICC's Arbitration Rules in effect at the time of filing the claim. The arbitral award of the ICC shall be binding on all parties and shall not be subject to appeal.

12.5 At the latest by 1 January 2024, EUROCONTROL, shall establish an independent, effective and impartial oversight supervisory body, as a functionally autonomous mechanism with the authority to issue binding instructions to EUROCONTROL, to handle complaints from Data Subjects.

From 1 January 2024, if the Data Subject believes EUROCONTROL did not resolve the complaint appropriately, he or she may lodge a complaint with the EUROCONTROL supervisory body mentioned in the preceding sentence for administrative redress.

12.6 From 1 January 2024, EUROCONTROL shall, , enable a data subject, who believes that his/her complaint was not resolved appropriately by the EUROCONTROL supervisory body mentioned in Article 12.5 above, to obtain effective redress and remedy, including compensation for material and non-material damages, before a permanent mechanism with compulsory jurisdiction that ensures independent and impartial *inter partes* adjudication, in accordance with the principles of due process, and whose decisions are binding on all parties and not subject to appeal., access to such mechanism shall be free of charge for the data subject.

12. 7 EUROCONTROL's obligations for the establishment of the supervisory body and the mechanism with compulsory jurisdiction mentioned in Articles 12.5 and 12.6 above, shall be subject to the approval of the EUROCONTROL Permanent Commission.

12.8 Each Party, shall handle and resolve in a reasonable and timely manner, and in any case within one month, extendable at maximum by two further months, a Data Subject complaint.

12.9 The Parties shall inform each other about complaints received from Data Subjects and the outcome of the proceedings.

12.10 Each Party may suspend or terminate the transfer of personal data until it considers the dispute as satisfactorily addressed. In case of such a suspension or termination, EUROCONTROL shall return or delete the transferred personal data and SESAR 3 JU shall notify such suspension or termination to the EDPS.

13 COOPERATION, NOTICES AND CORRESPONDENCE

13.1 Each Party, when so requested, shall provide a swift and efficient assistance to the other Party in execution of this DPAA.

13.2 The Parties shall meet regularly at least once per year and as required at the request of the other Party to discuss specific data protection, legal and technical issues.

13.3 Whenever responsibilities between Parties are not clear or not covered by this DPAA, the issue shall be discussed between the DPOs and legal team of the Parties, and reported if relevant to the periodical meeting.

13.4 In circumstances where responsibilities for Processors acting under the Parties' instructions require further clarification, this shall be discussed between the DPOs and legal team, and reported if relevant to the periodical meeting.

13.5 The SESAR 3 JU is subject to the scrutiny of the European Data Protection Supervisor in line with Article 58 of Regulation (EU) 2018/1725, which may apply its advisory, investigative and corrective powers in respect of the SESAR 3 JU when applicable. EUROCONTROL shall render the assistance required and provide all the information necessary for the SESAR 3 JU to comply with its obligations.

13.6 Designated officers for the cooperation under this article are:

For EUROCONTROL	For SESAR 3 JU
Hans Holderbach	Laura Gomez Gutierrez
Data Protection Officer	Data Protection Officer
Telephone: +32 2 729 5045	+32 2 507 80 59
hans.holderbach@eurocontrol.int	laura.gomez@sesarju.eu
data-protection-officer@eurocontrol.int	sju.data-protection@sesarju.eu

13.7 Contact points are mentioned, as applicable, for every specific processing operation, in the relevant privacy statements or respectively in the EUROCONTROL and SESAR 3 JU Data Protection Registers.

13.8 Any notices and correspondence given under or in relation to this DPAA shall be:
- in writing,
- signed by or on behalf of the Party giving it and
- served by delivering it personally "*in hand*", by sending it by pre-paid post, recorded delivery or registered post or by fax to the address and for the attention of the relevant Party notified for such purpose or to such other address as that Party may have stipulated in accordance with this Article.

Such notices and correspondence shall be effective at the time of delivery when delivered personally "*in hand*" or upon formal receipt by the other Party.

14 REVIEW OF THIS DATA PROTECTION ADMINISTRATIVE ARRANGEMENT - AMENDMENT

14.1 The Parties shall regularly discuss the practical, legal, technical and organisational aspects related to this DPAA according to the general provisions on cooperation and update this DPAA and its Annexes as appropriate.

14.2 The Articles of this DPAA may be modified only by an instrument in writing of equal formality, signed by the duly authorised representatives of both Parties after prior approval of the SESAR 3 JU Governing Board and authorisation of the European Data Protection Supervisor as per Article 48(3)(b) of Regulation (EU) 2018/1725.

14.3 The annexes of this DPAA may be modified by exchange of letters between the duly authorised representatives of both Parties as per Article 13.8 above.

14.4 SESAR 3 JU must assess any modification to the Annexes of this DPAA, together with its Data Protection Officer.

Where this assessment leads to a conclusion that the modification leads to substantial changes to the conditions of the EDPS authorisation of this DPAA under Article 48(3)(b) of Regulation (EU) 2018/1725, especially if it increases the risks to the rights and freedoms of data subjects resulting from the transfers, SESAR 3 JU must communicate such a modification in advance to the EDPS.

In this case, the modification cannot take effect before the EDPS decides if a new authorisation under Article 48(3)(b) of Regulation (EU) 2018/1725 is required.

15 SUPERVISION MECHANISM

15.1 Each Party shall conduct periodic reviews of its own policies and procedures that implement this DPAA and of their effectiveness and upon reasonable request by a Party, the other Party shall review its personal data processing policies and procedures to ascertain and confirm that the safeguards in this DPAA are being implemented effectively. The results of the review shall be communicated to the Party that requested the review.

15.2 In the event that the Receiving Party is unable to effectively implement the safeguards in this DPAA for any reason, it shall promptly inform the Transferring Party, in which case the Transferring Party shall temporarily suspend the transfer of personal data under this DPAA to the Receiving Party, until such time as the Receiving Party informs the Transferring Party that it is again able to act consistent with the safeguards. Each Party shall communicate such inability of a Receiving Party to effectively implement the safeguards in this DPAA to its respective supervisory authority.

15.3 The supervisory authority of a Party may at any point request the Party supervised by it to provide it with evidence concerning the compliance with this DPAA and take the actions necessary to remedy any processing activity that does not adhere to the standards and safeguards of this DPAA.

16 ENTRY INTO FORCE AND TERMINATION

16.1 This DPAA shall enter into force on the date of its adoption by the SESAR 3 JU Governing Board and take effect on the date on which the last Party signs it. Without prejudice to Article 16.2 below, the duration of this DPAA shall correspond to the duration of SESAR 3 JU as per Article 3(1) of the SBA.

16.2 Any Personal Data transferred from SESAR 3 JU to EUROCONTROL pursuant to this DPAA prior to its effective termination shall continue to be processed in accordance with the provisions set hereto.

SIGNATURES

For EUROCONTROL,

[redacted], Director General

signature: _____

Done at Brussels, on ……

For the SESAR 3 Joint Undertaking,

[redacted], Executive Director

signature:_____

Done at Brussels, on…….

Done in two copies, one for each Party, in English.

ANNEX I – PURPOSE, CATEGORIES OF DATA SUBJECT AND PERSONAL DATA, MAXIMUM RETENTION PERIOD FOR IDENTIFIED TRANSFERS OF PERSONAL DATA

1. TRANSFERS FROM SESAR 3 JU TO EUROCONTROL

A. Description of the purpose of the promotional, outreach and stakeholders relations activities referred to in articles 157(b) to (d) of the SBA, article 3 of the DPAA and Appendix 3.2 of the Administrative Agreement

1. The promotional activities shall include:

a) Interviews and features on/with SESAR 3 JU in Skyways, EUROCONTROL's magazine, or equivalent
b) Development of digital material (videos and animations) featuring specific solutions or interviews with SESAR 3 JU staff and project partners
c) Speaking slots for SESAR 3 JU representatives in EUROCONTROL events
d) Organisation of events at EUROCONTROL premises

2. Personal data collected and processed for this purpose shall relate to:

a) SESAR 3 JU staff
b) SESAR 3 JU stakeholders
c) Participants to the events

3. Data relating to the persons referred to in paragraph 2 may include only the following categories of personal data:

a) Name
b) Email address
c) Telephone number
d) Role in the organisation
e) Date of birth
f) Passport or ID card number
g) License plate (to grant access to the premises where the event is held)
h) Images/Video

4. Personal data referred to in paragraph 3 shall be retained for a maximum period of 5 years.

B. Description of the purpose of specialist support and advice - article 157(b) of the SBA, article 3 of the DPAA and Appendix 3.3 of the Administrative Agreement -

1. EUROCONTROL may provide technical support and advice to SESAR 3 JU projects. Personal data transferred to EUROCONTROL will be limited to name and contact details of participants involved in such projects.

2. Personal data collected and processed for this purpose shall relate to:

a) Project managers, coordinators and participants

3. Data relating to the persons referred to in paragraph 2 may include only the following categories of personal data:

a) Name
b) Email address
c) Function
d) Telephone number

4. Personal data referred to in paragraph 3 shall be retained for a maximum period of 5 years after the conclusion of the project.

C. Description of the purpose of Information Technology and related support services - article 157(g) of the SBA, article 3 of the DPAA, Appendices 4.1 and 4.2 of the Administrative Agreement-

1. EUROCONTROL provides some of the Information & Communication Technology services to the SESAR 3 JU in accordance with the SBA Article 157(g), which include:

a) Logical (re)configuration of assets/accounts/connections
b) Technical administration of the SESAR 3 JU systems and services to the extent necessary for the integrity of services provided
c) Provision of fixed and mobile telephone services including consumption
d) IT Service Desk (registration, diagnosis, tracking and resolution of incidents, creation/deletion of accounts, back-up restore and back-up services, restore services)
e) Wi-Fi Access (connection ID by user name)
f) Provisioning necessary hardware (user laptops, group printers, other peripherals like screens, keyboards, etc.)
g) Provisioning, installation and supporting of software
h) Provisioning, installation and supporting network services
i) IT Service management

The SESAR 3 JU Local Information Security Officer (LISO) can request further details of the security provisions applicable to the SESAR 3 JU and request changes that are necessary to secure compliance with the rules applicable to the SESAR 3 JU.

2. Personal data collected and processed for this purpose shall relate to:

a) SESAR 3 JU staff (all users with an IT user account)

3. Data relating to the persons referred to in paragraph 2 may include only the following categories of personal data:

a) Full name
b) Staff ID number
c) Email address
d) Assigned device (asset), type and number(s)
e) Printer usage
f) Security alerts
g) Work phone (fixed and/or mobile number)
h) Function in the SESAR 3 JU
i) Access rights granted by the SESAR 3 JU
j) IP addresses
k) Media Access Control (MAC) address of the assigned device
l) Mailing and Distribution lists
m) URL of visited websites

n) Meeting/call related data (outgoing and incoming telephone numbers, email addresses of meeting attendees, call/meetings dates/times, etc.)
o) Personal data provided by the user in order to facilitate the resolution of IT problems.

4. Personal data referred to in paragraph 3 shall only be retained for the minimum duration it is required for in support of the delivery of services to the individual, and in any case for maximum period of 5 year after the termination of the IT and related support services provided to SESAR 3 JU, on condition that no contentious issue occurred; in this case, data might be kept until this issue is resolved.

D. Description of the purpose of the logistics and infrastructure support - article 157(g) of the SBA, article 3 of the DPAA and Appendix 4.1 of the Administrative Agreement -

1. EUROCONTROL shall provide the logistics and facility services to SESAR 3 JU in accordance with SBA articles 157 (g) and 158. These services shall include provision of access badges to the non-restricted areas of EUROCONTROL headquarters and SESAR 3 JU offices

2. Personal data collected and processed for this purpose shall relate to:

a) SESAR 3 JU staff and
b) Visitors to SESAR 3 JU premises.

3. Data relating to the persons referred to in paragraph 2 may include only the following categories of personal data:

3.a. with reference to SESAR 3 JU Staff:

- First name, last name
- Date of birth
- Nationality
- Organisation (SESAR 3 JU)
- Start date and end date of assignment at EUROCONTROL HQ
- Vehicle number plate

3.b. with reference to visitors to the SESAR 3 JU premises:

- First name, last name
- Date of birth
- Nationality
- E-mail address
- Vehicle number plate
- Job and organisation and

4. Personal data referred to in paragraph 3 shall be retained for a maximum period of 1 year after the termination of the provision of the related service to SESAR 3 JU, on condition that no contentious issue occurred; in this case, data might be kept until this issue is resolved.

2. TRANSFERS FROM EUROCONTROL TO SESAR 3 JU

Description of the purpose of the functioning of the Programme Management Unit (PMU) - article 157(f) of the SBA, article 3 of the DPAA and Appendix 3.1 of the Administrative Agreement

1. The PMU will be managed by a PMU Head of Unit, who will be a member of EUROCONTROL staff and appointed by the Director General of EUROCONTROL, after approval of SESAR 3 JU Executive Director. The PMU Head of Unit will be placed under the administrative authority of EUROCONTROL but shall report operationally and functionally to SESAR 3 JU Executive Director. The PMU Head of Unit will determine, in coordination with SESAR 3 JU Executive Director, the roles and assignments they will carry out. EUROCONTROL and the SESAR 3 JU will agree in writing on the profile, qualifications and number of staff to be assigned to the PMU.

2. Personal data collected and processed for this purpose shall relate to:

a) EUROCONTROL staff members assigned to the PMU

3. Data relating to the persons referred to in paragraph 2 may include only the following categories of personal data:

a) Name
b) Email address
c) Mobile phone number (if applicable)

4. Personal data referred to in paragraph 3 shall be retained for a maximum period of 1 year after the termination of the data subjects' assignment to the PMU, on condition that no contentious issue occurred; in this case, data might be kept until the end of the legal procedure in progress.

3. RECIPROCAL TRANSFERS BETWEEN EUROCONTROL AND SESAR 3 JU

1. EUROCONTROL and SESAR 3 JU may transfer personal data of their staff for the purpose of administrating the Administrative Agreement and its schedules, especially through the coordination, steering and programme committees.

2. Personal data collected and processed for this purpose shall relate to:

a) EUROCONTROL staff members
b) SESAR 3 JU staff members

3. Data relating to the persons referred to in paragraph 2 may include only the following categories of personal data:

a) Name
b) Email address
c) Work phone number

4. Personal data referred to in paragraph 3 shall be retained for a maximum period of 1 year after the termination of the Administrative Agreement.

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES ENSURING SECURITY OF TRANSFERRED PERSONAL DATA

1 Technical and organisation measures common to all identified transfers of Annex I

1.1 Pseudonymisation and encryption (Art. 33 para. 1 lit a EUDPR) - Global measures that contribute to personal data confidentiality, integrity, and availability

A. Access control of processing areas.

Measures to prevent unauthorized persons from gaining physical access to the equipment where the Personal Data is processed:

- Access to premises is controlled by security guards and access control systems;
- Badge access to the data centre;
- CCTV is used both outside and within the facility and within the data centre where Personal Data is hosted;
- Protection and restriction of access paths;
- Established access authorizations for staff and third parties;
- Personnel Security Clearance requested for staff and third parties having access to the data centre where Personal Data is hosted ; and
- All access to the data centre where Personal Data are hosted is logged, monitored, and tracked.

B. Access control to data processing systems.

Measures to prevent its data processing systems from being abused by unauthorized persons:

- Authorised users are issued their own unique logins; passwords must adhere to constraints in length, complexity, aging and history. MFA is enforced when and where possible;
- Database security controls restrict access; controlled and audited;
- Automatic lock of user terminal if left idle, identification and password required to unlock;
- Automatic lock of the user account when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- Deactivation of user authentication credentials (such as user IDs) in case the person is disqualified from accessing Personal Data or in case of non-use for a substantial period of time, except for those authorized solely for technical management;
- Staff policies in respect of each staff access rights to Personal Data (if any), informing staff about their obligations and the consequences of any violations of such obligations; and
- Training of staff on data protection.

II. CONFIDENTIALITY (Art. 33 para. 1 lit b EUDPR)

A. Access control to use specific areas of data processing systems

Persons are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and Personal Data cannot be read, copied, modified, or removed without authorization:

- Staff members are assigned minimum access rights dependent on their job requirements (least privilege access principle);
- Staff policies in respect of each staff member's access rights to the Personal Data;

- Allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;
- Regular monitoring and update of authorization profiles;
- Release of data to only authorized persons as required;
- Policies controlling the retention of backup copies; and
- Use of state-of-the-art encryption technologies.

B. Separation of processing for different purposes
Measures to make sure that data collected for different purposes can be processed separately.

This is accomplished by:

- Access to data shall be separated through application security for the appropriate users;
- At the database level, data is stored in different areas, separated per module or function they support; and
- Interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

III. INTEGRITY (Art. 33 para. 1 lit b EUDPR)

A. Input control
Measures to establish whether and by whom personal data has been inputted into data processing systems or removed. This is accomplished by:

- Protective measures against data alteration in memory, storage (data at rest) and during transmission (data in motion).

B. Transmission Control
Measures to prevent the Personal Data from being altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- Use of state-of-the-art encryption technologies;
- All data transmissions are logged and monitored; and
- Monitoring of the completeness and correctness of the transfer of data (end-to-end check).

IV. AVAILABILITY AND RESILIENCE (Art. 33 para. 1 lit b EUDPR)

Measures to make sure that personal data is protected from; or can be recovered from accidental destruction or loss. This is accomplished by:

- Redundant uninterruptible power supply (UPS);
- Use of air-conditioning, temperature and humidity controls (monitored 24x7);
- Use of state-of-the-art protection technologies such as anti-virus and firewall;
- Use of state-of-the-art data protection technologies such as High Availability clusters, Raid and Snapshots;
- Daily Backups;
- Disaster recovery plans;
- Point in time backups are stored off-site and available for restore in case of failure;
- Regular check of all the implemented and herein described security measures;
- Backups are only re-used if information previously contained is not intelligible and cannot be reconstructed by any technical means; other removable media is destroyed or made unusable if not used; and

- Any detected security incident is recorded, alongside the followed data recovery procedures.

2 Specific technical and organisation measures

Not applicable to the transfers identified under Annex I of this DPAA.

ANNEX III – IDENTIFIED ONWARD TRANSFERS FROM EUROCONTROL TO RECIPIENTS

Purpose of the onward transfer	Ground for the onward transfer pursuant to article 3 of the DPAA	Categories of personal data to be onward transferred	Recipients or categories of recipients to which personal data will be onward transferred	Country where they are located or international organisation of which they are part
Webex support	Art. 3.d of the DPAA	Annex I B.3	INTRADO Contract ref : 19-110095-C-1-2 (Lot 1 and 2)	USA