INFORMATION NOTICE ON THE PROCESSING OF PERSONAL DATA REGARDING THE TRIAL-TESTING OF A FACE-RECOGNITION SYSTEM FOR PASSENGER ACCESS TO SECURITY AND BOARDING GATES AT VENICE MARCO POLO AIRPORT - SEAMLESS JOURNEY PROJECT

In accordance with Art. 13 of EU Reg. 2016/679 (GDPR), SAVE S.p.A., as Data Controller, provides passengers who voluntarily wish so, to "opt in" to allow information on personal data processing to be used as part of the trial-testing at Venice Marco Polo Airport of an innovative IT system (the "**System**") that uses face-recognition technology to identify passengers at checkpoints, to facilitate their access to security checkpoints and to the boarding gates, thus reducing waiting and transit times at checkpoints (the "**Seamless Journey Project**").

1. Data Controller

The Data Controller is the company **SAVE S.p.A.**, with registered office in Venice Tessera (VE), Via Galileo Galilei No. 30/1, VAT No. IT 02193960271 (herein referred to as the "**Company**" or " **Data Controller**").
The Company has appointed a Personal Data Protection Officer/Data Protection Officer (DPO), who can be contacted at the following email address: dpo@grupposave.com.

2. Subjects Concerned

Passengers departing from Venice Marco Polo Airport who decide to voluntarily join the Seamless Journey Project illustrated below by giving specific consent to the processing of their data.

3. Description of the Seamless Journey Project and its Data Processing

The process enabling passengers to board the aircraft involves passing through several airport checkpoints (check-in, air-side security checkpoints, boarding gates). At each checkpoint, passengers required to show their identification document and/or boarding pass. The verification of these documents is prescribed by current regulations to ensure safe and punctual transit to the aircraft. The need to present the documents at the various checkpoints makes the path leading to the passenger's boarding a smooth one.
The Seamless Journey Project aims to test-trial an automated identification system that allows passengers to register their data only once, thus speeding up transit at the subsequent checkpoints. Passengers who voluntarily opt into the Seamless Journey trial register at dedicated kiosks or check-in desks. The dedicated devices will associate the biometric characteristics of the passenger's face, specially detected by a camera, which will create a biometric face-image template, with the relevant identity document and boarding pass, creating a provisional "digital identity" that will allow passengers to be automatically recognised at the security checkpoints and at the boarding gate, enabling them to pass through the relevant checkpoints without having to show identity documents and boarding passes again. The image of a passenger's face captured by the system will not be recorded in any way, and will only be used instantaneously to generate the above-mentioned biometric template, i.e. an artificial image showing only the biometric contours of the face. The passenger's "digital identity" created in this way - as well as the personal data acquired for this purpose - will be deleted after flight departure and in any case within 24 hours of its acquisition.
The System operates through the phases of:

- **Enrolment**: involving the registration or "enrolment" of passengers and is carried out through the devices located at special kiosks or at specific counters check-in dedicated to this purpose. The passenger presents their passport, which is scanned through a reader (passport scanner) so that the System acquires their identification data and processes a biometric template of the facial features detected by the photo ID on the passport. In parallel, a camera installed on the device captures a real-time image of the passenger's face which it will use to process a second biometric template.
  During the enrolment phase, the system compares the first biometric template taken from the face image captured in real time by the camera with the second biometric template taken from the passport photo. If the System detects a match between the two biometric templates (i.e. recognises that the scanned ID belongs to the person who is registering), the enrolment is successful; if not, the passenger will have to repeat their enrolment. The image of the face acquired by the system will not be recorded in any way but will only be used instantaneously to generate the aforementioned biometric template, which is an artificial image showing only the face's biometric contours. The system thus constructs a provisional 'digital identity' of the passenger, created by associating the passport photo with the image of the passenger's face acquired in real time. The digital identity created during the enrolment phase is saved internally in the System for re-use in subsequent phases.
  The enrolment phase can be carried out by the passenger in two ways:
  - in automatic mode, at dedicated stations (kiosks) (in this case it is called 'automatic enrolment' because the passenger carries out the enrolment independently); or
  - in assisted mode, at the check-in counters with the assistance of a dedicated operator, who asks the passenger to provide their passport and then to stand in front of a camera (this is called 'assisted enrolment').
- **Reconciliation**: after the enrolment phase follows the reconciliation phase: passengers are asked to stand in front of a (face pod) camera that captures their face image and automatically compares it with the digital identities recorded by the System. If the reconciliation finds a match between the digital identity and the face image that has just been acquired, the passenger is asked to present their boarding card: in this way, the passenger's digital identity is enriched with the boarding-card data. Considering that enrolment phase and reconciliation phase will be simultaneous, for reconciliation the System will use the face image already acquired during enrolment.
- **Screening (at security checkpoints)**: After the reconciliation phase, the passenger goes to the security checkpoints to access the boarding areas. Here the passenger is asked to stand in front of a (face pod) camera installed near the access gate. If the facial image acquired during screening finds a match with a digital identity in the System, the System will also autonomously retrieve the passport and boarding pass information associated to that identity, thus reconstructing all of the passenger's

data: personal details, flight identification data and time, boarding gate, etc. Once the passenger has been conclusively recognised, the System allows the passenger access through the gate without requiring further presentation of the previously-acquired documents.

- **Screening (at boarding gate)**: the passenger finally goes to the boarding gate where a new screening takes place in the same way as described in the point above: if the passenger's identity is recognised, access will be granted without requiring further documents to be showed.

When the entire process has been completed and the passenger has boarded the aircraft, the System deletes the passenger's data, i.e. their digital identity.

4. Type of data processed and purpose of processing

Using the electronic readers described above (face pod camera and passport scanner), the System acquires the following personal data:

(i) common personal data contained in the passport:
first name, surname, date and place of birth, gender, residence, nationality, digital photo of the passenger, passport number, date of issue and expiry;

(ii) travel data contained on the boarding pass:
number, date and time of flight, airport of departure and destination, airline, passenger's first and last name, assigned seat number;

(iii) image of passenger's face captured in real time by a (face pod) camera.
Please note that the System processes the image of the passenger's face by detecting and measuring its salient features so as to transform them into a numerical code (biometric template), which does not allow the image to be traced back to the originally-acquired image and/or reconstructed and that, following the successful comparison with the biometric template derived from the digital photo acquired from the recognition document, it is stored in encrypted form and transmitted, together with the data referred to in points (i) and (ii) above, to an electronic file in a server of SAVE, protected by high security measures.

The above-mentioned data are acquired and processed to allow the passenger to access the air-side areas of the airport and to then board the aircraft in an automated way, without needing to show identity documents and boarding pass again.

5. Legal basis of processing and provision of data

Opting into the trial of the System described above and the releasing the aforementioned personal and biometric data are entirely optional for departing passengers, who remain free to use the usual methods of access to airport gates by showing their passport and reading their boarding pass.

Failure to provide the data shall result in the inability to take part in the trial.

The legal basis for the processing of the passenger's biometric data referred to in no. 4 iii) (relating to the facial characteristics detected for facial recognition purposes) is:

- the consent of the passenger wishing to join the Seamless Journey Trials. The Data Subject's (passenger's) consent will be acquired in explicit form in the manner given in the registration process (Enrolment).

The legal bases for processing the other personal data referred to in No. 4 i) and ii) are:

- fulfilment of legal obligations, performance of a task in the public interest or in connection with the exercising of public authority in relation to the checks to be carried out to allow access to airport areas;
- executing the passenger's request to join the trials of the System and the provision of related services to fulfil the relative legal and administrative obligations and to pursue legitimate interests related to the performance by SAVE of organisational and technical works pertaining to the System's operation and security, the verification of the relative reliability, and the analysis and evaluation of the results of the trials.

6. Processing methods, data retention period and criteria

For the purposes illustrated, personal data are processed by electronic tools and mainly automated procedures. Data are collected by the System by special sensors capable of scanning documents (passport scanner and boarding card scanner) and faces (face pod). Once acquired, this data is first encrypted and then stored on databases protected with high security measures.

The data stored in encrypted form will only be used for verifying the passenger's identity when passing through the gates dedicated to experimentation and equipped with the same face-recognition technology (highlighted with a specific infographic), located before the security checkpoints and the boarding gates, so that the data regarding the identification document and boarding pass that enable access to the aforesaid gates and/or the use of the services provided therein can be extracted and automatically checked.

Personal data acquired and used for System operation, including biometric data, will be deleted after the departure of the flight on which the passenger has boarded, and in any case no later than 24 hours after its acquisition.

Before deletion, the data collected will be made anonymous (i.e. stripped of personal information) for storage in anonymous form for statistical-analysis purposes. In fulfilment of the security obligations incumbent on the Data Controller as airport operator, data concerning the passing of airport gates will be stored (gate code, date and time of passing).

7. Communication of data to third parties - Recipients of data

The Company may communicate the processed data for the above purposes:

i) to internal company subjects;
ii) to companies responsible for airport security in their capacity as Data Processors;
iii) to service providers of technologies and software and hardware equipment that SAVE uses for rolling out the trials and technical activities of System installation, management and maintenance appointed as Data Processors;

iv) to Public Authorities, including the judiciary and law-enforcement authorities, in response to any requests for information required by law (e.g. Border Police, Carabinieri, Guardia di Finanza, Customs, ENAC, Prefecture, Local Health Authority, etc.).

8. Transfer of data to Third Countries

The processed data will not be transferred by the Data Controller to Third Countries (i.e. non-EU countries). However, in the event of any transfer of data to such countries, the transfer will take place in compliance with the regulations in force from time to time on the transfer of data to Third Countries.

9. Rights of the Data Subject, Withdrawal of Consent, and Complaint to the Supervisory Authority

The Data Subject has the right at any time to request personal-data access, rectification, erasure, and restriction, to object to the processing, and to exercise their right to data portability. The exercising of the Data Subject's rights will in any case take place in a way compatible with the characteristics of the personal-data processing.

As long as the processing continues, the Data Subject has the right to withdraw their consent to the processing of their data at any time without, however, affecting the lawfulness of the processing based on the consent given before such withdrawal.

In the event of an alleged breach, Data Subjects also have the right to lodge a complaint with a Data Protection Supervisory Authority in the EU Member State where they have their habitual residence, or in the EU Member State where they work, or where the alleged breach occurred.

10. Profiling and automated decision making

The processing is not carried out by automated decision making (e.g. profiling).

11. Contacts and requests

For a complete list of the Data Protection Contact Person appointed for each area and activity, and of the Data Processors/for further information on the transfer of data to non-EU countries, the mechanisms and safeguards for data transfer as per Art. 44 ff. GDPR/ to exercise the revocation of any consent you may have given or to exercise your rights (access, rectification, cancellation, restriction, opposition, portability), you may send a request to the following e-mail address: privacy@grupposave.com.