













**INFORMATION REGARDING THE PROCESSING OF PERSONAL DATA IN CASE OF BOARDING USING FACIAL RECOGNITION TECHNOLOGY AS PER ART. 13 and 14 of REG. (EU) 2016/679 ("GDPR")**

	<b>DATA CONTROLLER</b>					
The Data Controller of the process is: <b>S.A.C.B.O. S.p.A.</b> , Address: Via Orio al Serio 49/51 – 24050 Grassobbio (BG); e-mail address: <a href="mailto:privacy@sacbo.it">privacy@sacbo.it</a>						
	<b>DATA PROTECTION OFFICER (DPO)</b>					
The Data Controller has appointed a Data Protection Officer (DPO): <b>Partners4Innovation</b> c/o SACBO S.p.A., e-mail address: <a href="mailto:dpo@sacbo.it">dpo@sacbo.it</a>						
	<b>TYPES OF DATA PROCESSED</b>					
<p>If you choose the boarding method using facial recognition technology, S.A.C.B.O. S.p.A. will process the following personal data that you provide:</p> <ul style="list-style-type: none"> <li>➤ Identity card or Passport (which contain a document identification code, your name, your surname, your photograph and the document expiry date);</li> <li>➤ Boarding Pass and the data it contains (date and flight number you booked, airline, seat number and sequence number) which are necessary to enable the usual airport checks and a consistency check between the data shown in your identity document and your boarding pass;</li> <li>➤ Biometric data related to the characteristics of your face: the image of your face taken from your identity document or your passport to compare with the biometric model of your face, acquired through a system that captures facial traits, by measuring them and transforming them into a numerical code which cannot be traced back to the original image that was acquired and which, following a positive comparison with the image obtained from the digital photo acquired from the identity document, is saved in encrypted form and transmitted to an electronic archive held on an S.A.C.B.O. S.p.A. Server, which is protected to a high security level (S.A.C.B.O. S.p.A. is in possession of ISO 27.001 IT security certification).</li> </ul>						
	<b>SOURCE OF DATA</b>					
Personal data collected through your boarding pass is acquired by third-party companies, such as airline companies.						
	<b>DATA PROCESSING PURPOSES</b>	 <b>LEGAL BASIS</b>	 <b>DATA RETENTION PERIOD</b>			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; vertical-align: top; padding: 5px;"> <p>Personal data is acquired and processed for the sole purpose of streamlining and speeding up the identification operations as required by the applicable legislation and in relation to security checks, for the purpose of flight boarding.</p> <p>The collection of personal data will be adequate, pertinent and limited to the extent necessary with respect to the purpose, in accordance with the principles of minimization, necessity and proportionality of the data processing.</p> </td> <td style="width: 33%; vertical-align: top; padding: 5px;"> <p>The legal basis for the processing is your explicit consent</p> </td> <td style="width: 33%; vertical-align: top; padding: 5px;"> <ul style="list-style-type: none"> <li>➤ Personal data related to your boarding pass will be deleted as soon as your flight takes off and therefore it will be stored, encrypted, for the time that elapses from registration in the system until your flight takes off.</li> <li>➤ The identity document or passport data that is acquired during the registration phase at the airport is stored in two ways: <ul style="list-style-type: none"> <li>- in relation to each flight, data will be stored for the time that elapses between registration and take off and, in any case, for a period of time that is always less than 24 hours;</li> <li>- in the case of registration of a “frequent flyer”, subject to specific consent, the data will be stored for a period of time that does not exceed 12 months.</li> </ul> </li> <li>➤ The facial recognition data acquired during registration is stored in two ways: <ul style="list-style-type: none"> <li>- in relation to each flight, subject to specific consent, data will be kept in encrypted form for the time that elapses between airport registration and take off and, in any case, for a period of time that is always less than 24 hours;</li> <li>- in the case of registration of a “frequent flyer”, subject to specific consent, the data will be kept encrypted for a period of time that does not exceed 12 months.</li> </ul> </li> </ul> </td> </tr> </table>				<p>Personal data is acquired and processed for the sole purpose of streamlining and speeding up the identification operations as required by the applicable legislation and in relation to security checks, for the purpose of flight boarding.</p> <p>The collection of personal data will be adequate, pertinent and limited to the extent necessary with respect to the purpose, in accordance with the principles of minimization, necessity and proportionality of the data processing.</p>	<p>The legal basis for the processing is your explicit consent</p>	<ul style="list-style-type: none"> <li>➤ Personal data related to your boarding pass will be deleted as soon as your flight takes off and therefore it will be stored, encrypted, for the time that elapses from registration in the system until your flight takes off.</li> <li>➤ The identity document or passport data that is acquired during the registration phase at the airport is stored in two ways: <ul style="list-style-type: none"> <li>- in relation to each flight, data will be stored for the time that elapses between registration and take off and, in any case, for a period of time that is always less than 24 hours;</li> <li>- in the case of registration of a “frequent flyer”, subject to specific consent, the data will be stored for a period of time that does not exceed 12 months.</li> </ul> </li> <li>➤ The facial recognition data acquired during registration is stored in two ways: <ul style="list-style-type: none"> <li>- in relation to each flight, subject to specific consent, data will be kept in encrypted form for the time that elapses between airport registration and take off and, in any case, for a period of time that is always less than 24 hours;</li> <li>- in the case of registration of a “frequent flyer”, subject to specific consent, the data will be kept encrypted for a period of time that does not exceed 12 months.</li> </ul> </li> </ul>
<p>Personal data is acquired and processed for the sole purpose of streamlining and speeding up the identification operations as required by the applicable legislation and in relation to security checks, for the purpose of flight boarding.</p> <p>The collection of personal data will be adequate, pertinent and limited to the extent necessary with respect to the purpose, in accordance with the principles of minimization, necessity and proportionality of the data processing.</p>	<p>The legal basis for the processing is your explicit consent</p>	<ul style="list-style-type: none"> <li>➤ Personal data related to your boarding pass will be deleted as soon as your flight takes off and therefore it will be stored, encrypted, for the time that elapses from registration in the system until your flight takes off.</li> <li>➤ The identity document or passport data that is acquired during the registration phase at the airport is stored in two ways: <ul style="list-style-type: none"> <li>- in relation to each flight, data will be stored for the time that elapses between registration and take off and, in any case, for a period of time that is always less than 24 hours;</li> <li>- in the case of registration of a “frequent flyer”, subject to specific consent, the data will be stored for a period of time that does not exceed 12 months.</li> </ul> </li> <li>➤ The facial recognition data acquired during registration is stored in two ways: <ul style="list-style-type: none"> <li>- in relation to each flight, subject to specific consent, data will be kept in encrypted form for the time that elapses between airport registration and take off and, in any case, for a period of time that is always less than 24 hours;</li> <li>- in the case of registration of a “frequent flyer”, subject to specific consent, the data will be kept encrypted for a period of time that does not exceed 12 months.</li> </ul> </li> </ul>				
Once the retention terms indicated above have elapsed, the Data will be destroyed, deleted or made anonymous, compatibly with the technical cancellation and backup procedures						

	<b>PROVISION OF PERSONAL DATA</b>
<p>Pursuant to art. 13, co. 2, lit. e) of the GDPR, S.A.C.B.O. S.p.A informs you that the provision of personal and biometric data by departing passengers is entirely optional. Departing passengers remain free to use the usual methods of accessing airport departure gates, by having the boarding pass and the identity document or passport read by an airport operator, following the conventional procedure.</p> <p>The processing of a passenger's biometric data related to facial characteristics, which are necessary for the purpose of facial recognition, can only be carried out by S.A.C.B.O. S.p.A. if the passenger who intends to use the biometric detection system has given his or her consent.</p>	
	<b>AUTOMATED PROCESS</b>
<p>Opting for identification by means of facial recognition technology implies that identity checking is carried out automatically (validity of your identity document, correspondence with boarding card data and correspondence between the image in your identity document and your face).</p> <p>In the event that the identification process does not have a positive outcome, then boarding operations will be carried out with the usual conventional methods.</p>	
	<b>AUTHORIZED SUBJECTS TO THE PROCESSING</b>
<p>Data may be processed by employees of the corporate functions responsible for the pursuit of the purposes, who have been authorized to process and who have been received adequate operating instructions.</p>	
	<b>DATA RECIPIENTS</b>
<p>Personal data may be communicated to subjects operating as independent Data Controllers (such as, by way of example, Supervisory and Control Authorities and any public entity entitled to request the data) or processed, on behalf of the Company, by subjects designated as Data Processors, to whom adequate operating instructions are given (such as, by way of example, companies, consultants or professionals that S.A.C.B.O. S.p.A uses to deliver its services, including, in particular, the supplier responsible for the development and technical management of the facial recognition system).</p> <p>Personal data will be subjected to the highest security standards and will be stored exclusively in encrypted form. In no case will Personal Data be disclosed or, in any case, communicated to an indeterminate number of subjects.</p> <p>Personal data shall not be transferred to entities in Countries outside the EU.</p>	
	<b>RIGHTS OF THE DATA SUBJECT AND RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY</b>
<p>By contacting the Company via e-mail at <a href="mailto:privacy@sacbo.it">privacy@sacbo.it</a>, data subjects have the right to ask the Data Controller for access to data concerning themselves, the right to ask for erasure, rectification of inaccurate data, integration of incomplete data, restriction of the data processing as per art. 18 GDPR, as well as opposition to processing, for reasons related to their particular situation, in the hypothesis of legitimate interest of the Data Controller.</p> <p>Furthermore, if the data processing is based on consent or on a contract, and it is processed with automated tools, data subjects shall have the right to receive their personal data in a structured, commonly used and machine-readable format, as well as, if technically possible, have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided.</p> <p>Data subjects have the right to revoke the consent given at any time, as well as to oppose the processing carried out to pursue the legitimate interest of the Data Controller.</p> <p>Data subjects have the right to lodge a complaint to the competent Supervisory Authority in the European State in which they reside habitually or work, or the State in which the alleged data breach has occurred.</p>	