

VIDEO SURVEILLANCE INFORMATION

- Users video-monitored areas -

Airport Terminal

SO.GE.A.AL. S.p.A., the legal representative pro tempore, (hereinafter also referred to as “owner” or “company”) as required by current legislation (art. 13 General Data Protection Regulation, hereinafter also referred to as GDPR), provides users with information regarding the processing of their data acquired through the installed video surveillance system.

WHO IS THE OWNER AND HOW CAN THEY BE CONTACTED

The Data Controller is SO.GE.A.AL. S.p.A., with a registered office in Regione Nuraghe Biancu, 07041 Alghero (SS), Italy.

VAT number 01635090903.

The company can be contacted via email at privacy@sogeaal.it.

It should be noted that the Border Police use the video surveillance system for the autonomous purposes of public order and public security, pursued by the authority, the images captured through the system are viewed by its staff present in the operating room.

HOW TO CONTACT THE DATA PROTECTION OFFICER

The Data Controller has appointed the Data Protection Officer. They can be contacted at the following address:

SO.GE.A.AL. S.p.A.- Data Protection Officer, Nuraghe Biancu Region, Airport

Alghero-Fertilia, 07041 Alghero (SS), Italy email: dpo@sogeaal.it

WHAT DATA IS PROCESSED?

The data processed are the images acquired through the installed video surveillance system.

WHAT ARE THE PURPOSES AND LEGAL BASIS OF THE PROCESSING?

The processing of data collected through the video surveillance system is carried out for:

- Airport Security (understood in the dual meaning of safety, as a form of protection of the safety of persons involved in aviation operations, that of security, as a form of prevention and neutralisation of unlawful acts of interference which may be put in place against the system of

civil aviation at the airport and on-board aircraft).

- Protection of corporate assets and defensive needs.

The aforementioned purposes are pursued in accordance with the principles of correctness and lawfulness and in compliance with the legal provisions on the protection of personal data. The legal basis of the processing: with reference to the protection of the company's assets, the detection of defensive needs and its legitimate interest; with reference to airport Security, it is the legal obligation (deriving from the PNS - National Security Program); in the case of specific requests of law enforcement agencies and of the judicial authority, it is a legal obligation to respond.

The purposes mentioned above are pursued by the principles of correctness and lawfulness and in compliance with the legal provisions on protecting personal data. The legal basis of the processing: regarding the protection of the company's assets, the detection of defensive needs and its legitimate interest; regarding airport security, it is the legal obligation (deriving from the PNS - National Security Program); in the case of specific requests it is the legal obligation, of law enforcement agencies and the judicial authority.

DATA ACCESS

The data may be known explicitly by authorized internal personnel. The external subjects of which the Data Controller uses, who may know the data being processed are: those who provide assistance and maintenance of the system in the case of interventions that are necessary and that should require access to data and consultants for litigation management and legal assistance. The data may be transmitted to law enforcement and judicial authorities, in the case of specific requests to which the Data Controller is required, by law, to respond. The interested party may request from the Data Controller the list of external subjects who carry out activities as data processors. However, it should be noted that data communication is limited to only categories of data whose transmission is necessary for the performance of the activities and purposes pursued.

HOW DATA IS COLLECTED

The system allows both the recording and the real-time display of collected data. The processing is carried out through computer systems, and the display of the images is left to the explicitly authorised and trained personnel. The video surveillance system involves only processing personal data of subjects present in the areas taken. All video surveillance systems are indicated in respective areas by specific signs. The recordings of images are kept for seven days, except when it is necessary to adhere to a specific request of law enforcement and judicial authorities, so the data may be stored even beyond the terms indicated. The data is not disseminated or sent abroad.

WHAT HAPPENS IF THE DATA IS NOT PROVIDED?

The provision of data is optional and can be avoided by not accessing areas subject to video surveillance, which are indicated by signs placed to indicate the presence of cameras.

THE USERS RIGHTS

The law recognizes that the interested party has the right to ask the Data Controller for access to their personal data and the rectification or cancellation of data, the limitation or opposition to the processing of their data, as well as the right to data portability.

The aforementioned rights – for which further information is referred to below, can be exercised taking into account the intrinsic nature of the data collected. In particular, these are images collected in real-time concerning an objective fact. It should be noted that the right of updating, rectification or integration cannot be practically exercised and that the right to portability cannot be exercised, as provided for by the legislation if the processing is based on consent or on a contract and the processing is carried out by automated means.

The interested party may assert their rights at any time, without formalities, by contacting the Data Controller for the protection of personal data through the email address indicated. We will provide feedback in compliance with the terms of the law.

- **The right of access**, i.e. the right to obtain from the Data Controller the users confirmation as to the processing of personal data, to obtain access to the personal data and the following information: a) for the purposes of the processing; b) for the categories of personal data concerned; c) for the recipients or categories of recipients to whom the personal data has been or will be communicated, in particular for recipients of third countries or international organisations; d) when possible, the retention period of the personal data provided or, if not possible, the criteria used to determine such period; e) for the right to request from the Data Controller the rectification or erasure of personal data or restriction of processing of personal data concerning the user or to oppose the users processing; f) for the right to file a complaint with a supervisory authority; g) should all available information on their origin not be collected from the data subject h) for the existence of an automated decision-making process including profiling and, in those cases, meaningful information on the logic used, as well as the importance and the consequences expected of such processing for the data subject. Where personal data is transferred to a third country or an international organisation, the data subject has the right to be informed of adequate safeguards relating to the transfer.

- **The right of amendment** i.e. is the right to obtain from the Data Controller the rectification of inaccurate personal data without undue delay. Taking into account the purposes of the processing, the data subject has the right to obtain the integration of incomplete personal data, by providing an additional statement.

- **The right of erasure**, i.e. the right to obtain from the Data Controller the cancellation of personal data concerning the subject without undue delay if: a) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the subject revokes the consent on which the processing is based and if there is no other legal basis for the processing; c)

the subject opposes to the processing carried out because it is necessary for the performance of a task in the public interest or in the case of official authorities vested in the Owner or for the purposes of the legitimate interest and there is no legitimate reason prevailing to proceed with the processing, or opposes to the processing for direct marketing purposes; d) the personal data has been unlawfully processed; e) the personal data must be deleted in order to fulfil a legal obligation under Union or member state law to which the controller is subject; f) the personal data has been collected in relation to the provision of information society services to minors. However, the request for cancellation cannot be accepted if the processing is necessary: a) to exercise the right to freedom of expression and information; b) for the fulfilment of a legal obligation that requires processing provided by EU law or of the member state which is subject to the holder of the treatment or for the performance of a task carried out in the public interest or in the case of public authority vested in the holder of the processing; c) for reasons of public interest in the field of public health; d) for archiving purposes in the public interest, scientific research, historical, or statistical purposes, to the extent that the cancellation risks makes it impossible or seriously undermines the achievement of the objectives of that processing; e) for the assessment, exercise or defence rights in court.

- The **right of limitation**, i.e. the right to obtain processed data, except for storage, only with the consent of the data subject or for the assessment, exercise or defense of a right in court or to protect the rights of another natural or legal person or for reasons of important public interests of a union or of a member state, if: a) the interested party disputes the accuracy of the personal data, for the period needed by the Data Controller to verify the accuracy of such personal data; b) the processing is unlawful and the data subject objects to the erasure of personal data and instead requests that its use be limited; c) the Data Controller should no longer need this data for the purposes of processing, the personal data is necessary for the data subject to ascertain, exercise or defend a right in court; d) the interested party has opposed the treatment because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the owner or for the purposes of the legitimate interests of the holder of the treatment or of a third party, pending the verification on the possible prevalence of the legitimate reasons of the holder of the treatment compared to those of the data subject.

- The **right to portability**, i.e. the right to receive in a structured format, in common use and readable by automatic devices, personal data provided to the Data Controller. The Data Controller has the right to transmit data to another Data Controller without impediments from part of the holder who has supplied them, as well as the right to obtain the direct transmission of personal data by one Data Controller to another, if technically feasible, in cases where such processing is based on consent or on a contractual basis the processing is carried out by automated means. These rights shall be without prejudice for the right to erasure.

The **right to object**, i.e. the right of the interested party to oppose at any time, for reasons connected to their particular situation, to the processing of their personal data carried out because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the Owner or for the purposes of the legitimate interests of the holder of the treatment or of third parties. Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data carried out for these purposes, including profiling related to direct marketing.

VIDEO SURVEILLANCE INFORMATION

- Users video-monitored areas -
- Car parking system landside

SO.GE.A.AL. S.p.A., the legal representative pro tempore, (hereinafter also referred to as “owner” or “company”) as required by current legislation (art. 13 General Data Protection Regulation, hereinafter also referred to as GDPR), provides users with information regarding the processing of their data acquired through the installed video surveillance system.

WHO IS THE OWNER AND HOW CAN THEY BE CONTACTED

The Data Controller is SO.GE.A.AL. S.p.A., with a registered office in Regione Nuraghe Biancu, 07041 Alghero (SS), Italy.

VAT number 01635090903. The company can be contacted via email at privacy@sogeaal.it.

HOW TO CONTACT THE DATA PROTECTION OFFICER

The Data Controller has appointed the Data Protection Officer. They can be contacted at the following address:

SO.GE.A.AL. S.p.A.- Data Protection Officer, Nuraghe Biancu Region, Airport

Alghero-Fertilia, 07041 Alghero (SS), Italy email: dpo@sogeaal.it

WHAT DATA IS PROCESSED?

The data processed are the images acquired through the installed video surveillance system.

WHAT ARE THE PURPOSES AND LEGAL BASES OF THE PROCESSING?

The processing of data collected through the video surveillance system is carried out to protect the company's assets and defensive needs. The legal basis of the processing is the legitimate interest, which consists of protecting assets and persons and for defensive needs, as well as, the legal obligation in the case of specific requests of law enforcement and judicial authorities to respond. The purposes mentioned above are pursued by the principles of correctness and lawfulness and in compliance with the legal provisions on protecting personal data.

DATA ACCESS

The data may be known explicitly by authorized internal personnel. The external subjects of which the Data Controller uses, who may know the data being processed are: those who provide assistance and maintenance of the system in the case of interventions that are necessary and that should require access to data and consultants for litigation management and legal assistance. The data may be transmitted to law enforcement and judicial authorities, in the case of specific requests to which the Data Controller is required, by law, to respond. The interested party may request from the Data Controller the list of external subjects who carry out activities as data processors. However, it should be noted that data communication is limited to only categories of data whose transmission is necessary for the performance of the activities and purposes pursued.

HOW DATA IS COLLECTED

The system allows both the recording and the real-time display of collected data. The processing is carried out through computer systems, and the display of the images is left to the explicitly authorised and trained personnel. The video surveillance system involves only processing personal data of subjects present in the areas taken. All video surveillance systems are indicated in respective areas by specific signs. The recordings of images are kept for 24 hours, except when it is necessary to adhere to a specific request of law enforcement and judicial authorities, so the data may be stored even beyond the terms indicated. The data is not disseminated or sent abroad.

WHAT HAPPENS IF THE DATA IS NOT PROVIDED?

The provision of data is optional and can be avoided by not accessing areas subject to video surveillance, which are indicated by signs placed to indicate the presence of cameras.

THE USERS RIGHTS

The law recognizes that the interested party has the right to ask the Data Controller for access to their personal data and the rectification or cancellation of data, the limitation or opposition to the processing of their data, as well as the right to data portability.

The aforementioned rights – for which further information is referred to below, can be exercised taking into account the intrinsic nature of the data collected. In particular, these are images collected in real-time concerning an objective fact. It should be noted that the right of updating, rectification or integration cannot be practically exercised and that the right to portability cannot be exercised, as provided for by the legislation if the processing is based on consent or on a contract and the processing is carried out by automated means.

The interested party may assert their rights at any time, without formalities, by contacting the Data Controller for the protection of personal data through the email address indicated. We will provide feedback in compliance with the terms of the law.

- The **right of access**, i.e. the right to obtain from the Data Controller the users confirmation as to the processing of personal data, to obtain access to the personal data and the following information: a) for the purposes of the processing; b) for the categories of personal data concerned; c) for the recipients or categories of recipients to whom the personal data has been or will be communicated, in particular for recipients of third countries or international organisations; d) when possible, the retention period of the personal data provided or, if not possible, the criteria used to determine such period; e) for the right to request from the Data Controller the rectification or erasure of personal data or restriction of processing of personal data concerning the user or to oppose the users processing; f) for the right to file a complaint with a supervisory authority; g) should all available information on their origin not be collected from the data subject h) for the existence of an automated decision-making process including profiling and, in those cases, meaningful information on the logic used, as well as the importance and the consequences expected of such processing for the data subject. Where personal data is transferred to a third country or an international organisation, the data subject has the right to be informed of adequate safeguards relating to the transfer.

- The **right of amendment** i.e. is the right to obtain from the Data Controller the rectification of inaccurate personal data without undue delay. Taking into account the purposes of the processing, the data subject has the right to obtain the integration of incomplete personal data, by providing an additional statement.

- The **right of erasure**, i.e. the right to obtain from the Data Controller the cancellation of personal data concerning you without undue delay if: a) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the subject revokes the consent on which the processing is based and if there is no other legal basis for the processing; c) the subject opposes to the processing carried out because it is necessary for the performance of a task in the public interest or in the case of official authorities vested in the owner or for the purposes of the legitimate interest and there is no legitimate reason prevailing to proceed with the processing, or opposes to the processing for direct marketing purposes; d) the personal data has been unlawfully processed; e) the personal data must be deleted in order to fulfil a legal obligation under union or member state law to which the controller is subject; f) the personal data has been collected in relation to the provision of information society services to minors. However, the request for cancellation cannot be accepted if the processing is necessary: a) to exercise the right to freedom of expression and information; b) for the fulfilment of a legal obligation that requires processing provided by EU law or of the member state which is subject to the holder of the treatment or for the performance of a task carried out in the public interest or in the case of public authority vested in the holder of the processing; c) for reasons of public interest in the field of public health; d) for archiving purposes in the public interest, scientific research, historical, or statistical purposes, to the extent that the cancellation risks makes it impossible or seriously undermines the achievement of the objectives of that processing; e) for the assessment, exercise or defence rights in court.

- The **right of limitation**, i.e. the right to obtain processed data, except for storage, only with the consent of the data subject or for the assessment, exercise or defense of a right in court or to protect the rights of another natural or legal person or for reasons of important public interests of a union or of

a member state, if: a) the interested party disputes the accuracy of the personal data, for the period needed by the Data Controller to verify the accuracy of such personal data; b) the processing is unlawful and the data subject objects to the erasure of personal data and instead requests that its use be limited; c) the Data Controller should no longer need this data for the purposes of processing, the personal data is necessary for the data subject to ascertain, exercise or defend a right in court; d) the interested party has opposed the treatment because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the owner or for the purposes of the legitimate interests of the holder of the treatment or of a third party, pending the verification on the possible prevalence of the legitimate reasons of the holder of the treatment compared to those of the data subject.

- The **right to portability**, i.e. the right to receive in a structured format, in common use and readable by automatic devices, personal data provided to the Data Controller. The Data Controller has the right to transmit data to another Data Controller without impediments from part of the holder who has supplied them, as well as the right to obtain the direct transmission of personal data by one Data Controller to another, if technically feasible, in cases where such processing is based on consent or on a contractual basis the processing is carried out by automated means. These rights shall be without prejudice for the right to erasure.

The **right to object**, i.e. the right of the interested party to oppose at any time, for reasons connected to their particular situation, to the processing of their personal data carried out because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the owner or for the purposes of the legitimate interests of the holder of the treatment or of third parties. Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data carried out for these purposes, including profiling related to direct marketing.

The interested party is informed that if they consider the processing of their data occurs in violation of the provisions of the RGDP, they have the right to lodge a complaint with the guarantor, as provided for by art. 77 of the regulation itself or appeal to the appropriate courts (art. 79 of the law).

VIDEO SURVEILLANCE INFORMATION

- Users video-monitored areas - Aircraft apron area

SO.GE.A.AL. S.p.A., the legal representative pro tempore, (hereinafter also referred to as “owner” or “company”) as required by current legislation (art. 13 General Data Protection Regulation, hereinafter also referred to as GDPR), provides users with information regarding the processing of their data acquired through the installed video surveillance system.

WHO IS THE OWNER AND HOW CAN THEY BE CONTACTED

The Data Controller is SO.GE.A.AL. S.p.A., with a registered office in Regione Nuraghe Biancu, 07041 Alghero (SS), Italy.

VAT number 01635090903.

The company can be contacted via email at privacy@sogeaal.it.

HOW TO CONTACT THE DATA PROTECTION OFFICER

The Data Controller has appointed the Data Protection Officer. They can be contacted at the following address:

SO.GE.A.AL. S.p.A.- Data Protection Officer, Nuraghe Biancu Region, Airport

Alghero-Fertilia, 07041 Alghero (SS), Italy email: dpo@sogeaal.it

WHAT DATA IS PROCESSED?

The data processed are the images acquired through the installed video surveillance system.

WHAT ARE THE PURPOSES AND LEGAL BASIS OF THE PROCESSING?

The processing of data collected through the video surveillance system is carried out for:

- Airport operational and safety purposes (aimed at verifying the correct assignments of aprons to aircraft and the orderly movement of vehicles and personnel on the apron in order not to interfere with aircraft operations);
- Protection of corporate assets and defensive needs.

The aforementioned purposes are pursued in accordance with the principles of correctness and lawfulness and in compliance with the legal provisions on the protection of personal data. The

legal basis of the processing: with reference to the protection of the company's assets, the detection of defensive needs and its legitimate interest; with reference to airport Safety, it is the legal obligation (deriving from the PNS - National Security Program).

DATA ACCESS

The data may be known explicitly by authorized internal personnel. The external subjects of which the Data Controller uses, who may know the data being processed are: those who provide assistance and maintenance of the system in the case of interventions that are necessary and that should require access to data and consultants for litigation management and legal assistance. The interested party may request from the Data Controller the list of external subjects who carry out activities as data processors. However, it should be noted that data communication is limited to only categories of data whose transmission is necessary for the performance of the activities and purposes pursued.

HOW DATA IS COLLECTED

The system allows only the real-time display of collected data. The processing is carried out through computer systems, and the display of the images is left to the explicitly authorised and trained personnel. The video surveillance system involves only processing personal data of subjects present in the areas taken, All video surveillance systems are indicated in respective areas by specific signs. The data is not disseminated or sent abroad.

WHAT HAPPENS IF THE DATA IS NOT PROVIDED?

The provision of data is optional and can be avoided by not accessing areas subject to video surveillance, which are indicated by signs placed to indicate the presence of cameras.

THE USERS RIGHTS

The law recognizes that the interested party has the right to ask the Data Controller for access to their personal data and the rectification or cancellation of data, the limitation or opposition to the processing of their data, as well as the right to data portability.

The aforementioned rights – for which further information is referred to below, can be exercised taking into account the intrinsic nature of the data collected. In particular, these are images collected in real-time concerning an objective fact. It should be noted that the right of updating, rectification or integration cannot be practically exercised and that the right to portability cannot be exercised, as provided for by the legislation if the processing is based on consent or on a contract and the processing is carried out by automated means.

The interested party may assert their rights at any time, without formalities, by contacting the Data Controller for the protection of personal data through the email address indicated. We will provide feedback in compliance with the terms of the law.

- The **right of access**, i.e. the right to obtain from the Data Controller the users confirmation as to the processing of personal data, to obtain access to the personal data and the following information: a) for the purposes of the processing; b) for the categories of personal data concerned; c) for the recipients or categories of recipients to whom the personal data has been or will be communicated, in particular for recipients of third countries or international organisations; d) when possible, the retention period of the personal data provided or, if not possible, the criteria used to determine such period; e) for the right to request from the Data Controller the rectification or erasure of personal data or restriction of processing of personal data concerning the user or to oppose the users processing; f) for the right to file a complaint with a supervisory authority; g) should all available information on their origin not be collected from the data subject h) for the existence of an automated decision-making process including profiling and, in those cases, meaningful information on the logic used, as well as the importance and the consequences expected of such processing for the data subject. Where personal data is transferred to a third country or an international organisation, the data subject has the right to be informed of adequate safeguards relating to the transfer.
- The **right of amendment** i.e. is the right to obtain from the Data Controller the rectification of inaccurate personal data without undue delay. Taking into account the purposes of the processing, the data subject has the right to obtain the integration of incomplete personal data, by providing an additional statement.
- The **right of erasure**, i.e. the right to obtain from the Data Controller the cancellation of personal data concerning you without undue delay if: a) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the subject revokes the consent on which the processing is based and if there is no other legal basis for the processing; c) the subject opposes to the processing carried out because it is necessary for the performance of a task in the public interest or in the case of official authorities vested in the owner or for the purposes of the legitimate interest and there is no legitimate reason prevailing to proceed with the processing, or opposes to the processing for direct marketing purposes; d) the personal data has been unlawfully processed; e) the personal data must be deleted in order to fulfil a legal obligation under union or member state law to which the controller is subject; f) the personal data has been collected in relation to the provision of information society services to minors. However, the request for cancellation cannot be accepted if the processing is necessary: a) to exercise the right to freedom of expression and information; b) for the fulfilment of a legal obligation that requires processing provided by EU law or of the member state which is subject to the holder of the treatment or for the performance of a task carried out in the public interest or in the case of public authority vested in the holder of the processing; c) for reasons of public interest in the field of public health; d) for archiving purposes in the public interest, scientific research, historical, or statistical purposes, to the extent that the cancellation risks makes it impossible or seriously undermines the achievement of the objectives of that processing; e) for the assessment, exercise or defence rights in court.

- The **right of limitation**, i.e. the right to obtain processed data, except for storage, only with the consent of the data subject or for the assessment, exercise or defense of a right in court or to protect the rights of another natural or legal person or for reasons of important public interests of a union or of a member state, if: a) the interested party disputes the accuracy of the personal data, for the period needed by the Data Controller to verify the accuracy of such personal data; b) the processing is unlawful and the data subject objects to the erasure of personal data and instead requests that its use be limited; c) the Data Controller should no longer need this data for the purposes of processing, the personal data is necessary for the data subject to ascertain, exercise or defend a right in court; d) the interested party has opposed the treatment because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the owner or for the purposes of the legitimate interests of the holder of the treatment or of a third party, pending the verification on the possible prevalence of the legitimate reasons of the holder of the treatment compared to those of the data subject.

- The **right to portability**, i.e. the right to receive in a structured format, in common use and readable by automatic devices, personal data provided to the Data Controller. The Data Controller has the right to transmit data to another Data Controller without impediments from part of the holder who has supplied them, as well as the right to obtain the direct transmission of personal data by one Data Controller to another, if technically feasible, in cases where such processing is based on consent or on a contractual basis the processing is carried out by automated means. These rights shall be without prejudice for the right to erasure.

The **right to object**, i.e. the right of the interested party to oppose at any time, for reasons connected to their particular situation, to the processing of their personal data carried out because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the owner or for the purposes of the legitimate interests of the holder of the treatment or of third parties. Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data carried out for these purposes, including profiling related to direct marketing.

The interested party is informed that if they consider the processing of their data occurs in violation of the provisions of the RGDP, they have the right to lodge a complaint with the guarantor, as provided for by art. 77 of the regulation itself or appeal to the appropriate courts (art. 79 of the law).

VIDEO SURVEILLANCE INFORMATION

- Users video-monitored areas -

Baggage screening area

SO.GE.A.AL. S.p.A., the legal representative pro tempore, (hereinafter also referred to as “owner” or “company”) as required by current legislation (art. 13 General Data Protection Regulation, hereinafter also referred to as GDPR), provides users with information regarding the processing of their data acquired through the installed video surveillance system.

WHO IS THE OWNER AND HOW CAN THEY BE CONTACTED

The Data Controller is SO.GE.A.AL. S.p.A., with a registered office in Regione Nuraghe Biancu, 07041 Alghero (SS), Italy.

VAT number 01635090903.

The company can be contacted via email at privacy@sogeaal.it.

HOW TO CONTACT THE DATA PROTECTION OFFICER

The Data Controller has appointed the Data Protection Officer. They can be contacted at the following address:

SO.GE.A.AL. S.p.A.- Data Protection Officer, Nuraghe Biancu Region, Airport
Alghero-Fertilia, 07041 Alghero (SS), Italy email: dpo@sogeaal.it

WHAT DATA IS PROCESSED?

The data processed are the images acquired through the installed video surveillance system.

WHAT ARE THE PURPOSES AND LEGAL BASIS OF THE PROCESSING?

The processing of data collected through the video surveillance system is carried out for:

- Airport Security (understood in the dual meaning of safety, as a form of protection of the safety of persons involved in aviation operations, that of security, as a form of prevention and neutralisation of unlawful acts of interference which may be put in place against the system of civil aviation at the airport and on-board aircraft).

- Protection of corporate assets and defensive needs. The aforementioned purposes are pursued in accordance with the principles of correctness and lawfulness and in compliance with the legal provisions on the protection of personal data. The legal basis of the processing: with reference to the protection of the company's assets, the detection of defensive needs and its legitimate interest; with reference to airport Security, it is the legal obligation (deriving from the PNS -

National Security Program); in the case of specific requests of law enforcement agencies and of the judicial authority, it is a legal obligation to respond.

DATA ACCESS

The data may be known explicitly by authorized internal personnel. The external subjects of which the Data Controller uses, who may know the data being processed are: those who provide assistance and maintenance of the system in the case of interventions that are necessary and that should require access to data and consultants for litigation management and legal assistance. The data may be transmitted to law enforcement and judicial authorities, in the case of specific requests to which the Data Controller is required, by law, to respond to. The interested party may request from the Data Controller the list of external subjects who carry out activities as data processors. However, it should be noted that data communication is limited to only categories of data whose transmission is necessary for the performance of the activities and purposes pursued.

HOW DATA IS COLLECTED

The system allows both the recording and the real-time display of collected data. The processing is carried out through computer systems, and the display of the images is left to the explicitly authorised and trained personnel. The video surveillance system involves only processing personal data of subjects present in the areas taken. All video surveillance systems are indicated in respective areas by specific signs. The recordings of images are kept for seven days, except when it is necessary to adhere to a specific request of law enforcement and judicial authorities, so the data may be stored even beyond the terms indicated. The data is not disseminated or sent abroad.

WHAT HAPPENS IF THE DATA IS NOT PROVIDED?

The provision of data is optional and can be avoided by not accessing areas subject to video surveillance, which are indicated by signs placed to indicate the presence of cameras.

THE USERS RIGHTS

The law recognizes that the interested party has the right to ask the Data Controller for access to their personal data and the rectification or cancellation of data, the limitation or opposition to the processing of their data, as well as the right to data portability.

The aforementioned rights – for which further information is referred to below, can be exercised taking into account the intrinsic nature of the data collected. In particular, these are images collected in real-time concerning an objective fact. It should be noted that the right of updating, rectification or integration cannot be practically exercised and that the right to portability cannot be exercised, as provided for by the legislation if the processing is based on consent or on a contract and the processing is carried out by automated means.

The interested party may assert their rights at any time, without formalities, by contacting the Data Controller for the protection of personal data through the email address indicated. We will provide feedback in compliance with the terms of the law.

- **The right of access**, i.e. the right to obtain from the Data Controller the users confirmation as to the processing of personal data, to obtain access to the personal data and the following information: a) for the purposes of the processing; b) for the categories of personal data concerned; c) for the recipients or categories of recipients to whom the personal data has been or will be communicated, in particular for recipients of third countries or international organisations; d) when possible, the retention period of the personal data provided or, if not possible, the criteria used to determine such period; e) for the right to request from the Data Controller the rectification or erasure of personal data or restriction of processing of personal data concerning the user or to oppose the users processing; f) for the right to file a complaint with a supervisory authority; g) should all available information on their origin not be collected from the data subject h) for the existence of an automated decision-making process including profiling and, in those cases, meaningful information on the logic used, as well as the importance and the consequences expected of such processing for the data subject. Where personal data is transferred to a third country or an international organisation, the data subject has the right to be informed of adequate safeguards relating to the transfer.

- **The right of amendment** i.e. is the right to obtain from the Data Controller the rectification of inaccurate personal data without undue delay. Taking into account the purposes of the processing, the data subject has the right to obtain the integration of incomplete personal data, by providing an additional statement.

- **The right of erasure**, i.e. the right to obtain from the Data Controller the cancellation of personal data concerning you without undue delay if: a) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the subject revokes the consent on which the processing is based and if there is no other legal basis for the processing; c) the subject opposes to the processing carried out because it is necessary for the performance of a task in the public interest or in the case of official authorities vested in the Owner or for the purposes of the legitimate interest and there is no legitimate reason prevailing to proceed with the processing, or opposes to the processing for direct marketing purposes; d) the personal data has been unlawfully processed; e) the personal data must be deleted in order to fulfil a legal obligation under Union or member state law to which the controller is subject; f) the personal data has been collected in relation to the provision of information society services to minors. However, the request for cancellation cannot be accepted if the processing is necessary: a) to exercise the right to freedom of expression and information; b) for the fulfilment of a legal obligation that requires processing provided by EU law or of the member state which is subject to the holder of the treatment or for the performance of a task carried out in the public interest or in the case of public authority vested in the holder of the processing; c) for reasons of public interest in the field of public health; d) for archiving purposes in the public interest, scientific research, historical, or statistical purposes, to the extent that the cancellation risks makes it impossible or seriously undermines the achievement of the objectives of that processing; e) for the assessment, exercise or defence rights in court.

- The **right of limitation**, i.e. the right to obtain processed data, except for storage, only with the consent of the data subject or for the assessment, exercise or defense of a right in court or to protect the rights of another natural or legal person or for reasons of important public interests of a union or of a member state, if: a) the interested party disputes the accuracy of the personal data, for the period needed by the Data Controller to verify the accuracy of such personal data; b) the processing is unlawful and the data subject objects to the erasure of personal data and instead requests that its use be limited; c) the Data Controller should no longer need this data for the purposes of processing, the personal data is necessary for the data subject to ascertain, exercise or defend a right in court; d) the interested party has opposed the treatment because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the owner or for the purposes of the legitimate interests of the holder of the treatment or of a third party, pending the verification on the possible prevalence of the legitimate reasons of the holder of the treatment compared to those of the data subject.

- The **right to portability**, i.e. the right to receive in a structured format, in common use and readable by automatic devices, personal data provided to the Data Controller. The Data Controller has the right to transmit data to another Data Controller without impediments from part of the holder who has supplied them, as well as the right to obtain the direct transmission of personal data by one Data Controller to another, if technically feasible, in cases where such processing is based on consent or on a contractual basis the processing is carried out by automated means. These rights shall be without prejudice for the right to erasure.

The **right to object**, i.e. the right of the interested party to oppose at any time, for reasons connected to their particular situation, to the processing of their personal data carried out because it is necessary for the performance of a task for public interest or in the exercise of official authority vested in the Owner or for the purposes of the legitimate interests of the holder of the treatment or of third parties. Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data carried out for these purposes, including profiling related to direct marketing.

The interested party is informed that if they consider the processing of their data occurs in violation of the provisions of the RGDP, they have the right to lodge a complaint with the guarantor, as provided for by art. 77 of the regulation itself or appeal to the appropriate courts (art. 79 of the law).