Privacy Policy

Code: EGN_CC_PL.01_R.03

Date issued: May 2025

EGNATIA AVIATION

General

Department	Type	No	Kind	Version		
Corporate Compliance	PL	01	-	03		
Title	Owner:	Approved by:	Applies to:	Effective date	Last reviewed	Next review
Privacy Policy	Corporate Compliance	C-Suite	All staff	05/2025	05/2026	05/2027
Relevant documents:			1. EGN_CC_PL.02_R.02_Security Policy 2. EGN_CC_PL.03_R.02_Personal Data Processing Policy (WIFI, CCTV) 3. EGN_CC_PL.04_R.02_Clean desk Policy 4. EGN_CC_PL.05_R.02_Electronic Media Access & Control Policy 5. EGN_CC_PL.06_R.02_Email Use Policy			

Scope

This Policy applies to all departments and personnel of the Company, as well as to any natural or legal person processing personal data on behalf of the Company, including partners, suppliers, and external service providers. The Policy concerns the processing of personal data of customers, suppliers, partners, and other third parties within the context of the Company's activities.

The Policy is reviewed at least annually and, on an ad hoc basis, in the event of material changes to the applicable legal and regulatory framework, to the processing activities, to the information systems, or to the Company's organizational structure, as well as in the event of personal data breach incidents or significant findings arising from audits or compliance assessments.

Purpose

On 25 May 2018, the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" (hereinafter: the "GDPR") entered into force, establishing rules relating

to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of such data.

EGNATIA AVIATION (hereinafter: the "Company") places particular emphasis on ensuring the protection of personal data. The Company recognizes that the protection of personal data constitutes an essential element of its lawful and secure operation and is committed to processing personal data in accordance with the GDPR, applicable national legislation, and the principles of accountability.

The main purposes of this Policy are as follows:

- to declare the Company's commitment to the most effective management of personal data, particularly through information technology means,
- to provide general guidance on personal data protection issues related to the collection, use, processing, disclosure, monitoring, etc., of the personal data it processes,
- to define the fundamental requirements that must be observed when processing personal data, taking into account the provisions of the GDPR and the relevant national law.

Definitions

Systems: All information systems and their databases, physical records, other digital records, operating software, application software, and computer functions within the organization, including indicatively central processing units of information networks, personal desktop and portable computers, workstations and servers, telecommunications equipment (routers, bridges, etc.), emerging technologies under development, as well as any other specialized computer systems operating in functional units where data are transmitted, distributed, or processed via electronic, telecommunications, satellite, microwave, or other means.

Data Controller: The natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processing: Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Data Processor: The natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller, as defined above.

Data Protection Impact Assessment (DPIA): An assessment of the impact of the envisaged processing operations on the protection of personal data, carried out by the Data Controller prior to processing, where a type of processing, in particular using new technologies and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

Data Subject: An identifiable natural person whose identity can be determined, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject").

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Special Categories of Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Policy Description

Principles Governing the Processing of Personal Data

Whenever the Company processes personal data, it always applies the following principles, according to which:

i) Personal data shall be processed lawfully and fairly **("lawfulness, fairness and transparency")**.

ii) Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those purposes **("purpose limitation")**.

The purposes for which personal data are processed must be communicated to the Data Subjects in the form of a written privacy notice, provided at the time of collection in clear and simple language. Personal data must be processed only for the purposes communicated to the Data Subjects and must not be processed in a manner incompatible with those purposes.

iii) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **("data minimization")**.
Only the personal data that are strictly necessary for achieving the purposes communicated to the Data Subjects shall be collected and processed.

iv) Personal data must be accurate and, where necessary, kept up to date **("accuracy")**

The Company shall maintain contact with the Data Subjects and periodically review their personal data. Personal data that are inaccurate, having regard to the purposes for which they are processed, must be erased or rectified without delay.

v) Personal data must not be kept for longer than is necessary for the purposes for which they are processed **("storage limitation")**.

Once the purposes of the processing have been fulfilled, personal data may be retained only in a form which does not permit identification of the Data

Subjects. Measures for the "de-identification" of personal data include deletion, encryption, redaction and anonymization, insofar as such measures do not conflict with other applicable laws and regulations.

vi) The processing of personal data must be carried out with respect for the rights of the Data Subject, as provided in Chapter III of the Regulation, which will be analysed in more detail below. Processing shall be carried out in a transparent manner vis-à-vis the Data Subjects and with respect for their rights, as provided for in Articles 12–22 GDPR **("transparency")**.

vii) Appropriate security measures must be taken with respect to personal data to protect them against unauthorized or unlawful processing and against accidental loss, destruction or damage **("integrity and confidentiality")**.

viii) Transfers of personal data outside the EU shall take place only where the conditions set out in Chapter V GDPR are met, in particular on the basis of an adequacy decision, appropriate safeguards (e.g. SCCs, BCRs), or, by way of exception, one of the derogations under Article 49 **("secure transfer")**.

Compliance with the above principles must always be demonstrated ("**accountability**") through the establishment of internal regulations, procedures and other measures, which may include the implementation of appropriate data protection policies by the Data Controller.

Whenever a specific processing of personal data takes place and the Company acts as Controller, the principles set out in this Chapter must be applied.

Legal Basis for Processing

The processing of personal data shall be lawful only if it is based on one of the legal bases provided for in Article 6 GDPR:

i) Processing is based on the consent of the Data Subject, which has been given for one or more specific purposes.

ii) Processing is necessary for the performance of a contract or in order to take steps at the request of the Data Subject prior to entering into a contract.

iii) Processing is necessary for compliance with legal obligations to which the Company is subject under the applicable legislation in force from time to time.

iv) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person, such as, for example, for the protection of the life or health of a natural person who is exposed to immediate risk, for monitoring epidemics and their spread, or in cases of natural and man-made disasters.

v) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

vi) Processing is necessary for the purposes of the legitimate interests pursued by the Company, except where such interests are overridden by the interests or the fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a minor (under 18 years of age).

CONSENT: Where processing is based on consent, the Company ensures that such consent is freely given, specific, up to date, informed, and demonstrable, and that it may be withdrawn as easily as it is given. In the context of employment, the Company does not, as a rule, rely on consent as a legal basis, unless, by way of exception, it can be demonstrated that such consent is indeed freely given in accordance with the GDPR and the applicable national legislation.

Information to be Provided to the Data Subject Regarding the Processing of Their Personal Data

The Company provides the required information in accordance with Articles 13 or 14 GDPR, depending on whether the data are collected from the Data Subject or from another source. This Policy does not replace the individual privacy notices applicable per category of Data Subjects or per processing activity. Data Subjects must be adequately and clearly informed of the personal data protection policy implemented by the Company and, in particular, of all details relating to the processing of their personal data, including, indicatively: i) the identity and contact

details of the Controller and, where applicable, of the Controller's representative, ii) the contact details of the Data Protection Officer, where applicable, iii) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing, iv) where processing is based on the legitimate interests pursued by the Controller or by a third party, the legitimate interests pursued, v) any recipients or categories of recipients of the personal data collected, vi) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period, vii) the rights of the Data Subject, viii) where processing is based on consent, the right to withdraw consent at any time, as well as the consequences of such withdrawal, ix) the right to lodge a complaint with the supervisory authority, as well as the address of the authority with which the complaint may be lodged, etc.

Exercise of Data Subjects' Rights

The Company shall respond to requests for the exercise of rights without undue delay and, in any event, within one (1) month of receipt thereof, unless the conditions for an extension pursuant to the GDPR are met. As a rule, and subject to certain conditions set out in the applicable regulations, the Company shall comply with and facilitate Data Subjects in exercising the following rights:

a) Right to access

The Data Subject shall have the right to obtain, at any time, confirmation from the Controller as to whether or not personal data concerning them are being processed and, where that is the case, access to such data shall be provided without undue delay.

b) Right to rectification

The Data Subject shall have the right to obtain from the Controller, without undue delay, the rectification of inaccurate or outdated personal data concerning them. They shall also have the right to have incomplete personal data completed, including by means of a supplementary statement. Furthermore, the Company undertakes to communicate any rectification of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or

involves disproportionate effort. The Company shall inform the Data Subject about those recipients if requested to do so.

c) Right to erasure («right to be forgotten»)

The Data Subject shall have the right to obtain from the Controller the erasure of personal data concerning them without undue delay.

d) Right to restriction of processing

The Data Subject shall have the right to obtain from the Controller restriction of processing of personal data concerning them. Where processing has been restricted, such personal data shall, with the exception of storage, be processed only where specific exceptions apply.

e) Right to data portability

The Data Subject shall have the right to receive the personal data concerning them, which they have provided to a Controller, in a structured, commonly used and machine-readable format.

f) Right to object

The Data Subject shall have the right to object, at any time and on grounds relating to their particular situation, to the processing of personal data concerning them where such processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller, or where processing is necessary for the purposes of the legitimate interests pursued by the Controller. Where the right to object is exercised, the personal data shall no longer be processed unless compelling legitimate grounds for the processing are demonstrated which override the interests, rights and freedoms of the Data Subject, or for the establishment, exercise or defence of legal claims. The Company guarantees that, where the Data Subject objects to the processing of personal data concerning them, such data shall no longer be processed unless it demonstrates compelling legitimate grounds for the processing which override the interests and rights of the Data Subject.

g) Automated individual decision-making, including profiling

The Data Subject shall have the right to object to a decision based solely on automated processing, including profiling, where such decision produces legal effects concerning them or similarly significantly affects them. The Company does not, as a rule, implement processes involving solely automated decision-making that produce legal effects or similarly significantly affect Data Subjects. Should this change, a specific compliance assessment shall be carried out in advance and appropriate information shall be provided to the Data Subjects.

Finally, the Company shall ensure overall that:

- Procedures are defined and adopted to enable the easy exercise of Data Subjects' rights, so that all required actions are carried out promptly.
- Data Subjects receive information regarding the actions taken.
- Data Subjects are informed of the details on how to exercise the above rights.
- The exercise of rights is provided free of charge, unless the request is manifestly unfounded or excessive, in particular due to its repetitive character, in which case the Company may charge a reasonable fee or refuse to act, in accordance with the GDPR.

Data Protection by Design and by Default (privacy by design and privacy by default)

In order to ensure the implementation of the above-mentioned principles and requirements, as well as the fulfilment of the rights of Data Subjects, the Company shall adopt appropriate technical and organizational measures in an effective manner.

The principle of data protection by design is based on the concept that it is preferable to build personal data processing means in accordance with appropriate technical and organisational measures from the outset of the design process, rather than attempting to adapt a product or service at a later stage. Participation in the design process supports the consideration of the entire data lifecycle and its use.

Where new procedures or transactions are envisaged, these shall be assessed in a documented manner also from a personal data protection perspective, in order to

ensure that all appropriate measures have been identified and, consequently, implemented as soon as the execution of such new procedures or transactions commences (data protection by design).

The Company shall adopt appropriate technical and organizational measures to ensure, by default, that only personal data which are necessary for each specific purpose of processing are collected (data protection by default). This obligation also applies with regard to the extent of personal data collected, the scope of their processing, the period of their storage, and their accessibility. Furthermore, such measures shall ensure that, by default, personal data are not made accessible, without human intervention, to an indefinite number of natural persons.

Whenever applications, services, and products involving the processing of personal data are developed, designed, selected, and used, due consideration must be given to issues relating to personal data protection (such as, for example, the principles referred to above).

The assessment of the principles of privacy by design and privacy by default is triggered, in particular, when a new information system is introduced, when the vendor changes, when a new form or a new website flow is created, when monitoring mechanisms or closed-circuit television (CCTV) systems are implemented, as well as when new technology is used or large-scale processing of personal data is carried out. In all such cases, it is required that data protection principles be embedded from the design stage and that, by default, the highest possible level of personal data protection is ensured.

Record of Processing Activities

The Company shall maintain and update a record of processing activities in accordance with Article 30 GDPR. This record shall be kept in writing, including in electronic form, and shall be made available to the Hellenic Data Protection Authority upon its request.

Where the Company acts as Controller, the record shall include, as a minimum, following information:

i) the name and contract details of the Controller and, where applicable, of the joint Controller and the Data Protection Officer,

ii) the purposes of the processing,

iii) a description of the categories of Data Subjects and of the categories of personal data,

iv) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations,

v) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where necessary, documentation of appropriate safeguards,

vi) where possible, the envisaged time limits for erasure of the different categories of data,

vii) where possible, a general description of the technical and organisational security measures in place.

Where the Company acts as Processor, the record shall include, as a minimum, the following information:

i) the name and contact details of the Processor(s) and of each Controller on behalf of which the Company is acting, as well as of the Data Protection Officer,

ii) the categories of processing carried out on behalf of each Controller,

iii) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where necessary, documentation of appropriate safeguards,

iv) where possible, a general description of the technical and organisational security measures in place.

Where the Company acts as a Processor on behalf of Controllers, it shall create and maintain specific record for each Controller.

Adoption and Implementation of Appropriate Technical and Organisational Measures to Ensure a Level of Security Appropriate to the Risk

The Company adopts and implements appropriate technical and organisational measures in order to ensure the required level of security of personal data, in accordance with the principle of accountability.

The selection of such measures is based on a risk-based approach, under which, in particular, the likelihood and severity of the risk to the rights and freedoms of Data Subjects are assessed, taking into account the nature, scope, context and purposes of the processing, as well as the state of the art and the cost of implementation.

Indicatively, the Company implements measures such as pseudonymisation and encryption of data, ensuring the confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability of and access to data in a timely manner in the event of an incident, and regular testing, assessment and updating of the effectiveness of such measures.

The above measures are further specified in the Company's individual policies and procedures. More specifically, such measures are further detailed in the Company's individual policies and procedures, including, indicatively, the Security Policy, the Security Plan, the Access Control and Monitoring Policy for Electronic Communications Systems, the Email Policy, the Personal Data Processing Policy for Visitors (WiFi and CCTV), as well as in any relevant procedures for incident management, access control, risk management, and data retention implemented by the Company.

Notification of Personal Data Breaches to the Competent Supervisory Authority and to the Data Subject

Where a personal data breach is identified, the Company shall implement adequate procedures to ensure the proper management of such incidents. Each incident shall be assessed without undue delay as to whether it constitutes a personal data breach and as to the level of risk involved. Notification to the competent supervisory authority shall be made within 72 hours from the moment the Company becomes aware of the breach, unless the breach is unlikely to result in a risk to the rights and

freedoms of natural persons. Any notification made after the expiry of the 72-hour period must include a justification for the delay. Furthermore, in the event of a personal data breach that is likely to result in a high risk to the rights and freedoms of Data Subjects, the Company shall communicate the personal data breach to the Data Subject without undue delay.

Transfer of Personal Data to Third Countries or International Organisations – Required Safeguards for Transfers Outside the EEA

The Company shall transfer personal data outside the EEA only where:
a) an adequacy decision of the European Commission exists; or
b) appropriate safeguards have been provided in accordance with Article 46 GDPR, in particular Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) or
c) by way of exception, one of the derogations under Article 49 GDPR applies.
Where required, the Company shall assess whether the laws and practices of the third country affect the level of protection and shall implement supplementary measures where necessary.

Designation of Processors

Prior to selecting a processor, it shall be ensured that the processor has implemented appropriate technical and organisational measures capable of ensuring compliance with the principles and requirements for the protection of personal data, as well as the exercise of the rights of Data Subjects. In particular, the processor shall maintain a record of processing activities, appoint a Data Protection Officer where required, provide sufficient guarantees, carry out due diligence, and enter into processor agreements containing all mandatory elements. In the event of transfers of personal data outside the EU, the processor shall apply the safeguards described above. It shall also be ensured that persons authorised to process personal data have committed themselves to confidentiality obligations or are under an appropriate statutory obligation of confidentiality.
Whenever a third party is selected to perform activities involving the processing of personal data, a contract shall be concluded between the Company and the

processor, governing their relationship and applicable thereafter. The written designation of the processor and the conclusion of such contract are essential in order for both parties to understand their responsibilities and obligations. The processor agreement shall include, at a minimum, the subject matter, duration, nature and purpose of the processing, the type of personal data and the categories of Data Subjects, as well as the obligation of the processor to process the data solely on the basis of documented instructions from the Controller. Furthermore, it shall include confidentiality obligations, the implementation of appropriate technical and organisational measures (TOMs), clear terms governing the use of sub-processors, as well as the obligation of the processor to assist the Controller in fulfilling Data Subject rights, conducting Data Protection Impact Assessments (DPIAs), and managing personal data breaches (breach handling). Finally, the contract shall regulate the return or deletion of data upon termination of the provision of services, as well as audit rights and the provision of information demonstrating compliance.

The Company shall designate only processors that can provide sufficient guarantees that the requirements of the GDPR will be met and that the rights of Data Subjects will be protected.

Furthermore, the Company shall ensure that processors act only on its documented instructions and process personal data in accordance with this Policy and the applicable data protection laws and regulations.

Accountability

The Company shall ensure that it is able to demonstrate compliance with the principles relating to privacy and the protection of personal data. For this purpose, clear responsibilities, internal and external audits, and controls over all personal data processing activities shall be established and maintained.

The Company is required to document and demonstrate the existence of recorded procedures and practices aimed at addressing data protection issues at an early stage, both during the development of information systems and in the handling of personal data breaches. The Company shall appoint a Data Protection Officer where required by the GDPR or where deemed necessary in the context of its organizational compliance.

The principle of accountability provides that the more likely and the more severe the risks associated with a given processing activity, the more stringent the measures that must be taken to mitigate them. The Company shall take into account factors that may render processing high-risk, such as:

- risks that may result in discrimination, identify theft or fraud,
- risks that may cause reputational damage or any other economic or social disadvantage,
- Risks associated with special categories of data and/or large-scale processing of personal data.

Data Minimisation

The Company shall limit the collection and processing of personal data to those that are adequate, relevant, and strictly necessary for the purposes pursued.

It shall adopt appropriate technical and organisational measures to ensure compliance with the principle of data minimisation:
i) at the stage of data collection, so that no more data than those adequate, relevant, and strictly necessary for the purposes of the Controller are collected; and
ii) at the stage of processing, so that, if data that are not adequate, relevant, and strictly necessary for the purposes of the Company have been collected, they are not subject to further processing operations. To this end, the Company shall periodically assess whether a specific category or categories of data remain adequate, relevant, and strictly necessary for each individual lawful processing purpose, resulting in the deletion or anonymisation of personal data as soon as they are no longer necessary for the achievement of the respective purpose.

The Company shall ensure that personal data undergoing processing are:

- adequate – sufficient to properly fulfil the stated purpose,
- relevant – logically connected to that purpose, and
- limited to what is strictly necessary (i.e. no more data are held than required for that purpose).

Third Parties

In the course of its activities, the Company shall share personal data with third parties. Such parties include public, international or private entities, as well as external service providers. Service providers include contractors, maintenance and repair providers of equipment, cloud service providers, network service providers, application and internet service providers, and other organisations providing information systems development.

For the transfer of such personal data, the Company shall:

i) Establish defined roles, responsibilities, and data protection access requirements for external service providers.

ii) Incorporate GDPR requirements for the protection of personal data and privacy into the relevant contracts.

iii) Revise contracts used for the procurement of IT goods and services to include specific GDPR requirements for data protection and privacy in agreements with external IT product and service providers.

iv) Ensure that the transfer of personal data to third parties takes place only where necessary for a defined and lawful processing purpose, is based on an appropriate legal basis, and is documented in accordance with the principle of accountability.

v) Include in memoranda of understanding, letters of intent, or similar agreements with third parties a detailed description of the personal data transferred and the purposes for which they may be used.

vi) Monitor, control, and train personnel regarding the authorised exchange of personal data with third parties and the consequences of unauthorised use or disclosure.

vii) Assess any proposed new data sharing with third parties in order to evaluate potential impacts on data protection and whether additional or new privacy notices are required.

Processing of Employees' and Candidates' Personal Data – Specific Rules

The privacy and protection of employees' personal data is of particular importance to the Company. The Company processes personal data of employees and job

applicants only to the extent necessary for purposes related to recruitment, the management of the employment relationship, compliance with legal obligations, the protection of its legitimate interests, and the security of its premises and systems, in accordance with the GDPR and applicable employment and national legislation. Consent is not, as a rule, used as the primary legal basis in the employment context, except by way of exception, where it can be demonstrated that it is freely given.

This section supplements the more specific notices and procedures implemented by the Company within the framework of the employment relationship. This Policy describes the manner in which the Company will manage employees' personal data in relation to their employment or prospective employment. The Company may, from time to time, update its Data Protection Policy to ensure consistency with future developments, market trends and/or any changes in legal or regulatory requirements.

At regular intervals, it may be necessary for employees to provide the Company with personal data relating to themselves and other individuals, for purposes related to their employment or their application for employment with the Company.

Where an employee provides the personal data of a third party to the Company, the employee shall ensure that such disclosure is lawful, that the third party has been informed where required, and that an appropriate legal basis exists for the disclosure.

The Company may collect, use and/or disclose employees' personal data for the following purposes:

- assessment of suitability for recruitment to specific positions,
- determination, processing and review of salaries, incentives, remuneration and other benefits,
- evaluation of employee performance,
- review and processing of applications for continuous skills development and training, including participation in seminars, training programmes and staff development activities,
- provision of necessary resources and assistance to employees in relation to the performance of their duties (including, indicatively, travel arrangements on behalf of employees),

- provision of insurance schemes,
- monitoring compliance with the Company's internal rules and policies,
- protection and enforcement of the Company's contractual and legal rights and obligations,
- any other purpose specified in the employee–employer contract, in accordance with applicable law,
- any other purpose reasonably related to the above. Employees must ensure that all personal data submitted to the Company are complete, accurate, truthful and correct.

The specific purposes, corresponding legal bases, recipients, and retention periods for employee and candidate data are set out in a separate employee/candidate privacy notice, as reflected in the Employee Privacy Notice.

Security of Personal Data, Information and Communications

The Company shall carry out integrity and security controls to protect all computing and telecommunications systems, personal data and information, in order to prevent or mitigate:

i) unauthorised access, alteration and/or disclosure of data; and
ii) accidental loss, deletion or destruction of data.

Such controls are also intended to address risks arising from the potential misuse of information and telecommunications systems.

These controls shall include, inter alia, the following: access controls (operating systems, database systems, application software), network and access security, user identification and authentication, firewalls, cryptographic controls (encryption, hashing, etc.), communication controls (email, telecommunications, etc.), information classification methods, information retention and disposal, and a mechanism for monitoring, reporting and resolving security incidents and personal data breaches.

Security Standards

Information systems security standards define the minimum criteria, rules and procedures established by the Company's senior management and approved by the competent corporate body/management, which are required to ensure the implementation of the Company's Information Security Policy.

These shall be implemented by various personnel (e.g. security officer, system security officer, end users, IT department managers, system development staff, etc.) under the direction of Management. These persons shall specify in detail the requirements of each procedure and/or control to be implemented.

Core Requirements Applicable Where the Company Acts as Processor

In all cases where, in relation to a specific personal data processing activity, the Company acts as Processor, it shall comply with the following:

i) Process personal data in accordance with this Policy and applicable data protection laws and regulations.

ii) Ensure that persons authorised to process personal data are bound by confidentiality clauses or are subject to an appropriate statutory obligation of confidentiality.

iii) Process personal data only on the documented instructions of the Controller, unless otherwise required by applicable law.

iv) Maintain a record of all processing activities.

v) Implement appropriate technical and organizational measures to ensure the security of personal data processing.

vi) Appoint a Data Protection Officer where required.

vii) In the event of transfers of personal data outside the EU, apply the safeguards described above.

viii) Enter into a contract or other legal act governing the relationship with the Controller.

ix) Not engage another processor without the prior specific authorisation of the Controller. Where a general written authorisation has been obtained for the use of sub-processors, the Controller shall be informed of any intended changes concerning the addition or replacement of sub-

processors, thereby allowing the Controller to object to such changes.

x) Where engaging other processors to carry out specific processing activities on behalf of the Controller, enter into a contract with the new processor imposing the same data protection obligations as set out in the contract with the Data Controller.

xi) Undertake to assist the Controller in fulfilling its obligations regarding responses to requests relating to Data Subject rights.

xii) Assist the Controller in fulfilling its obligations, cooperating in a timely manner in carrying out Data Protection Impact Assessments (DPIAs) and assisting, where required, in prior consultation with the competent supervisory authority.

xiii) Promptly notify the Controller of any personal data breach or incident affecting personal data processed on behalf of the Controller.

xiv) Upon termination of services, at the choice of the Controller, return or delete all personal data and delete existing copies, unless Union or Member State law requires their retention. The Processor shall also make available to the Controller all necessary information to demonstrate compliance with its legal obligations and shall cooperate with audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

Storage Limitation of Personal Data

The Company shall retain personal data in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the data are processed, in compliance also with statutory obligations requiring data retention for specific periods. Data already collected for a specific purpose shall not be subject to further processing that is incompatible with the original purpose.

In order to comply with the obligation of limiting the storage period and processing duration, the Company shall classify personal data and shall predefine time limits for their deletion or periodic review, in accordance with a data retention schedule to be established. In this context, retention periods are defined per category of processing and documented in an appropriate record maintained and updated by the Company (Record of Processing Activities). These retention periods are

determined and substantiated based on applicable legal obligations, limitation periods for claims, contractual requirements, as well as accounting and tax obligations, or other regulatory requirements applicable on a case-by-case basis.

Data Protection Officer (DPO)

The Data Protection Officer shall act independently in the performance of their duties, report to the highest management level, and shall not receive instructions regarding the exercise of their tasks. The DPO shall also be supported by a team of personnel responsible for relaying relevant GDPR-related information from each department. The Data Protection Officer shall report to the highest management level, and the Company shall ensure that the DPO does not hold a position that allows them to determine the purposes and means of personal data processing.
The Data Protection Officer shall perform the following duties:

i) Inform and advise the Company and its staff who process personal data regarding their obligations under this Policy and other applicable data protection legislation.
ii) Monitor the Company's compliance with this Policy and other applicable legal provisions.
iii) Where requested, provide advice regarding the potential conduct of a Data Protection Impact Assessment (DPIA) and monitor its implementation.
iv) Act as the contact point for communication with Data Subjects and the competent supervisory authority on matters relating to personal data processing.

The Company has appointed as Data Protection Officer (DPO) an external associate, lawyer – specialised legal advisor in personal data protection matters, Zoi Athanasiadou, email: privacy@egnatia-aviation.com.

Awareness and Training

The Company's Management is responsible for ensuring the awareness and training of all employees and for promoting the implementation of best practices in the management of personal data. Particular priority is given to effective

communication and training. This includes the implementation of a sustainable privacy programme based on a strong awareness and training component. The Data Protection Officer, in cooperation with senior Management, shall ensure the implementation and maintenance of a consistent, properly supported and effective privacy protection programme.

The Data Protection Officer is responsible for developing, implementing and maintaining the privacy awareness and training plan. This plan shall document the process of training, education and awareness-raising on privacy matters and shall ensure that all employees understand their role in protecting the confidentiality, integrity and availability of personal data as assets of the Company.

In this context, staff training is mandatory upon recruitment and is repeated on a periodic basis to ensure continuous updating of knowledge. It is also tailored according to the role and responsibilities of each employee, taking into account their level of access to and processing of personal data. Participation in and completion of training is documented through appropriate attendance records and completion logs, which are systematically maintained by the Company.

The plan shall also define what information is communicated, when, to whom, who is responsible for communication, and the procedure through which such communication takes place.

Compliance and Consequences

All employees, partners, and third parties falling within the scope of this Policy are required to fully comply with its provisions, as well as with the applicable personal data protection legislation. The Company ensures the training and awareness of its personnel on data protection matters and monitors compliance through appropriate controls and procedures, including the conduct of regular internal audits on a semi-annual basis by the DPO.

Any breach of this Policy may result in the imposition of disciplinary measures, in accordance with applicable labour law and the Company's internal regulations, which may, as the case may be, extend up and including termination of the employment relationship. In the event of a breach by partners or third parties, the Company reserves the right to take appropriate contractual and/or legal measures.

Furthermore, non-compliance with the applicable regulatory framework may result in administrative sanctions, including fines, in accordance with the General Data Protection Regulation and applicable national legislation.
The competent supervisory authority is the Hellenic Data Protection Authority (1-3 Kifisias Avenue, GR-115 23 Athens, Tel.: +30 2106475600, e-mail: contact@dpa.gr).

Record Keeping

Records and data related to the implementation of this Policy include, indicatively, the Record of Processing Activities, records of data subject requests and corresponding responses, personal data breach records, Data Protection Impact Assessments (DPIAs), legitimate interest assessments, consent records where applicable, contracts and assessments of processors, records of transfers to third countries, staff training records, as well as the findings of internal compliance audits.

The above records are maintained in approved physical and/or electronic files and information systems of the Company, under the responsibility of the competent departments and under the supervision of the Data Protection Officer, where required. Access to such records is restricted to authorised persons, in accordance with their role and responsibilities and the principle of least privilege.

The records are retained for a period consistent with the Company's retention policies, operational needs, and applicable legal and regulatory obligations in force from time to time. Upon expiry of the relevant retention period, the records shall be securely deleted, destroyed, or anonymised, unless their further retention is required for compliance, audit, or for the establishment, exercise, or defence of legal claims.