DATA PROTECTION POLICY

ABSTRACT | Danaos Management Consultants S.A. and its affiliated companies (hereinafter Danaos) have established as a major objective the adoption of data protection principles and the permeation of all of their daily business operations with an acute data protection mentality. Danaos has consistently achieved compliance with the existing legal framework regarding data protection and undertaken the needful actions derived from the new elements that emerged from the repealing of DIRECTIVE 95/46/EC and Greek state law 2472/97 and the establishment of General data protection regulation 2016/679.

SCOPE | This policy applies to any personal data processing activities conducted by the personnel of Danaos, either as Data Controller or Data Processor**.**

PURPOSE | The purpose of this policy is to:

- Clarify Danaos' roles as defined by GDPR and relative Greek state laws.
- Communicate the data protection goals of Danaos to the organization's employees and all concerned parties.
- Communicate the principles which govern any personal data processing conducted by Danaos.
- Communicate that Danaos recognizes data subjects' rights and is willing to fulfill them.
- Communicate to Danaos employees their responsibilities regarding personal data processing.
- Declare the presence of data protection officer.

ROLES | By nature of its business operations, Danaos is considered:

- a Data Controller and Data Processor regarding any data processing activity conducted on its employees' personal data.
- a Data Processor regarding any data processing activity conducted following a request by any of its clients.

GOALS | Danaos aims to achieve the following data protection goals:

- Ensure that any processing activity conducted by Danaos employees respects data protection principles.
- Ensure compliance with all legal and statutory requirements both as a Data Controller and a Data Processor.
- Ensure the protection of the human rights defined in the Charter of Fundamental Rights (2000/C 364/01) and the ongoing assessment of the risks derived by new technologies and state-of-the-art threats.
- Take into consideration and update internal procedures according to any adopted opinion or guidelines provided by the Article 29 Working Party of DIRECTIVE 95/46/EC and the European Data Protection Board (EDPB).
- Assist any Data Controller/client with their compliance with the Data Protection Regulation or any relative legislation.
- Ensure that Danaos employees adhere to their responsibilities, adopt a data protection mentality and follow the procedures and organizational measures established and encouraged by management and the data protection officer.
- Ensure that Danaos employees adhere to the security and relevant thematic internal policies established by the IT Department, which constitute essential parts of the Information Security Management System (ISMS).

DATA PROTECTION PRINCIPLES | Any personal data processing activity conducted by Danaos, either as Data Controller or Data Processor, must be characterized by the following principles:

- Lawfulness and fairness

  Personal data must be collected and processed in a legal and fair manner. Any processing should be based on at least one of the legal bases defined in GDPR Article 6 or an institutionalized derogation.

- Transparency in relation to data subjects

  The data subject must be informed regarding how their data is processed in a concise, transparent and intelligible way.

- Purpose limitation

  Personal data must be processed lawfully and explicitly for the original purpose it has been collected.

- Data minimization

  The extent of personal data collection is relevant to the purpose of collection. Before processing any personal data, an assessment of proportionality to the purpose must be conducted.

- Accuracy

  In cases where personal data accuracy is necessary to fulfill the purpose of data processing, all of the necessary actions must be taken to ensure the validity of the data processed.

- Storage limitation

  Personal data that is no longer needed after the expiration of the legal or business process-related periods must be deleted.

- Security in terms of Confidentiality, Integrity and Availability

  The conditions under which personal data processing is conducted must eliminate the scenario of a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

DATA SUBJECTS RIGHTS

Danaos recognizes and is willing to help data subjects exercise without delay their rights related to personal data processing.

Any data subject whose data is processed by Danaos is able to exercise:

- The right to access

  Every data subject whose personal data is processed by Danaos, as Data Controller, has the right to obtain information regarding:

  1. The reason for which its personal identifiable information (PII) is being processed.
  2. The type/categories of personal identifiable information (PII) being processed.
  3. The recipients to whom the personal data has been or will be disclosed, if applicable.
  4. The envisaged period for which the personal data will be stored, or the criteria used to determine that period.
  5. The right to lodge a complaint with a supervisory authority.
  6. The source that provided the personal data to Danaos.

Once a data subject exercises its right to access, they will receive a copy of the personal data processed as long as the rights and freedoms of others are not adversely affected.

- The right to rectification

  Every data subject whose personal data is processed by Danaos, as Data Controller, has the right to obtain from Danaos without undue delay the rectification of inaccurate personal data concerning him or her.

- The right to erasure

  Every data subject whose personal data is processed by Danaos, as Data Controller, has the right to obtain from Danaos without undue delay the deletion of its personal data once it is no longer necessary in relation to the purposes for which it was collected unless either of the overriding conditions below are met:

  1. For compliance with a legal obligation which requires processing according to a Union or Member State law to which Danaos is subject.
  2. For the establishment, exercise or defense of legal claims.

- The right to restriction of processing

  Every data subject whose personal data is processed by Danaos, as Data Controller, has the right to request the restriction of processing if one of the following conditions are met:

  1. The accuracy of the personal data is contested by the data subject.
  2. Danaos no longer needs the personal data for the purposes of processing, but it is required by the data subject for the establishment, exercise or defense of legal claims.

- The right to object

  Danaos recognizes that any data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of their personal data which is based on the legitimate interests of Danaos. Once a data subject exercises its right to object, their data will not be processed until an assessment is conducted on whether the compelling legitimate grounds of processing do not infringe the interests, rights and freedoms of the data subject.

Danaos, as Data Processor, will assist any Data Controller/client with the fulfilment of their obligation to respond to requests for exercising data subjects' rights, as mandated in GDPR Article 28.

INFORMATION SYSTEMS SECURITY

Danaos has established state-of-the-art technical and organizational measures to ensure high levels of security, as interpreted by the Confidentiality, Integrity, Availability (C.I.A.) model. The IT Department is responsible for the maintenance of the Information Security Management System, particularly:

- Danaos has equipped its infrastructure with technologies such as Firewall, Cloud Antivirus, Proxy servers and network monitoring tools in order to eliminate any state-of-the-art threat and strictly follows update and software patching procedures.

- Danaos maintains a disaster recovery site to enhance the availability and resilience of its information systems and to ensure the Business Continuity of the organization.

- Danaos has verified that any software or protocol used for remote accessibility is not vulnerable and is up to date.
- Danaos has applied very detailed access control management on the information and software on its information systems.
- The Danaos IT Department has established technical and organizational measures to enhance the complexity of the authentication mechanisms within the Information System.

ASSET USE POLICY

Danaos employees must use the organization's assets explicitly and without exception only for the fulfillment of business purposes and the implementation of business tasks respective to their job description. all hardware and software assets fall under the scope of the use policy.

DATA BREACH TREATMENT

Danaos has established procedures, governed by the IT Department, to communicate any potential data breaches to the below entities according to GDPR Articles 33 and 34, suggestions of HDPA and WP29 guidelines:

- Data Controllers when Danaos acts as a Data Processor
- Hellenic Data Protection Authority (HDPA)
- Affected data subjects

RESPONSIBILITIES

Danaos employees must adhere to the organization's data privacy policy and follow the procedures and guidelines generated and encouraged by management, the IT Department and the data protection officer. In particular, and in order to ensure security, eliminate the infringement of data protection principles and enhance the levels of transparency and accountability, all employees must:

- Follow the documented security guidelines generated by the IT Department regarding their workstations and adhere to the relevant thematic policies.
- Adhere to the particular use policies on the organization's assets.
- Adhere to the clean desk policy in the working environment.
- Adhere to all documented internal procedures.
- Perform any remote support activity as explicitly described by the statutory agreement between the Data Controller (client) and Data Processor (Danaos).
- Explicitly follow the documented internal procedure established for cases where a maintenance task includes personal data transfer to Danaos' infrastructure.
- Register any remote data processing activity in the record of processing maintained by Danaos, in accordance with GDPR Article 30.
- Adhere to the confidentiality/non-disclosure agreement they have signed.
- Immediately report any potential data breach to the IT Department.
- Consult the data protection officer regarding any matter which is related to personal data processing even if it does not fall under the documented procedures.
- Consult the Quality Department regarding any access control matter on digital or physical files.

DATA PROTECTION OFFICER

- Data subjects whose personal data is processed by Danaos may contact the data protection officer with regard to all issues related to the processing of their personal data and to the exercise of their rights.

- Danaos employees may contact the data protection officer for any clarification regarding data protection principles and request guidelines in order to perform data processing in an optimum way and avoid potential infringement of the legislation.

- Data protection officer contact details:
  Email: **dataprotection@danaos.gr**
  Tel.: **+30 2104196612**