

Policy on personal data processing & Protection and use of communication means

Compliance | Business Ethics



ENERGY & UTILITIES



FOOD & SUPPLY



REAL ESTATE
MANAGEMENT



TRANSPORTATION
& INFRASTRUCTURE



TECHNOLOGY



POSTAL SERVICES

TABLE OF CONTENTS

1. INTRODUCTION - DEFINITIONS	3
2. KEY PRINCIPLES OF PROCESSING.....	3
3. CONDITIONS OF LAWFUL PROCESSING.....	4
4. SPECIAL CATEGORIES OF PERSONAL DATA	4
5. COOPERATION WITH THIRD PARTIES.....	4
6. TECHNICAL AND ORGANIZATIONAL MEASURES.....	5
7. USE OF COMMUNICATION MEANS - EQUIPMENT.....	6
8. RIGHTS OF DATA SUBJECTS.....	7
9. INFORMATION & ACCESS	7
10. RECTIFICATION	7
11. DELETION	7
12. RESTRICTION OF PROCESSING.....	8
13. OBJECTION.....	8
14. DATA PROTECTION OFFICER	8
15. TRAINING.....	8
16. COOPERATION WITH SUPERVISORY AUTHORITIES	8
17. COMPLETION – REVISION	9
PERSONAL COMMITMENT	10

1. Introduction - Definitions

Protecting the personal data of natural persons (the "Data Subjects") is a primary concern of the Hellenic Corporation of Assets and Participations S.A. ("the Company").

Personal Data is any information relating to an identified or identifiable natural person, such as name, home address, date of birth, marital status, financial information, etc.

In this context, the Company adopts this Policy, which sets the general guidelines for the processing of Personal Data in compliance with the applicable national and EU laws. It is noted that the term "processing" in this Policy has the meaning given to it by law, i.e. any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise, association or combination, restriction, erasure or destruction.

In exercising their duties, the Company's personnel as well as any person (Directors or Supervisory Board members, etc.) who have a certain relationship with the Company (the "Officers") are required to apply this Policy and the relevant laws. The Company's associates shall apply the legislation on the processing of the Personal Data of the Data Subjects and shall take into account this Policy to the extent that it concerns them based on the nature of the processing they have undertaken.

2. Key principles of processing

2.1. The Company and its Officers shall take all appropriate measures to ensure that Personal Data are:

- a) processed lawfully, fairly and in a transparent manner ("lawfulness, fairness and transparency");
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation");
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- d) accurate and, where necessary, updated ("accuracy");
- e) kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

2.2. Data Subjects provide their personal data to the Company only if requested by the Company.

3. Conditions of lawful processing

3.1. The Company processes Personal Data only if, and to the extent that, at least one of the conditions described in the law apply, including (without being limited to) the following:

- a) the Data Subject has consented to the processing of their personal data for the specific purpose;
- b) processing is necessary for the execution of an agreement to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into an agreement;
- c) processing is necessary for compliance with a legal obligation to which the Company is subject;
- d) processing is necessary for the performance of a task carried out in the public interest;
- e) processing is necessary for the purposes of the legitimate interests pursued by the Company or a third party;

In this context, the Company may transfer Personal Data as required, indicatively, to companies affiliated therewith, partners, public authorities, etc., in order to fulfil its contractual or legal obligations or otherwise in accordance with the above.

3.2. The consent of the Data Subject, if required, is granted at the time of Personal Data collection after having been informed, in accordance with the requirements of the law.

3.3. The withdrawal of the Data Subject's consent shall have no retroactive effect.

3.4. Company Officers must process the Personal Data for the above legitimate purposes and within the limits of permissible use set by the Company. The transfer of Personal Data to a third party should take place with a view to a specific purpose as above. Special attention should be paid where special categories of Data, in the sense of the law, need to be processed, such as health data, as well as where Personal Data need to be transferred outside Greece.

3.5. Company Officers must not accept Personal Data from the Company's associates, unless they have understood and confirmed the legal basis and the purpose of processing such Personal Data.

4. Special categories of personal data

4.1. The Company processes special categories of Personal Data, in the sense of the law, such as health data, so far as one of the requirements stipulated by law applies, namely the Data Subject has given explicit consent to this; the processing is necessary for the fulfilment of obligations and the exercise of specific rights of the Company or the Data Subjects arising from the labour and social security law; the processing is necessary for the establishment, exercise or support of legal claims, etc.

5. Cooperation with third parties

5.1. The Company may cooperate with third parties, natural or legal persons, to whom it may be required to transfer Personal Data in order for such third parties to fulfil their obligations arising from the contractual relationship.

5.2. When processing is to be performed on behalf of the Company by third-party processors, the Company shall use processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that ensure the protection of the rights of the Data Subject according to the requirements of the law.

5.3. The relevant contract shall include terms regarding the Personal Data processing purpose and method as well as the rights and obligations of the parties, in general, as required by the applicable law. The personnel of the Company's associate who processes Personal Data on behalf of the Company, during the contract term, shall be bound by an appropriate confidentiality statement.

5.4. The criteria of Personal Data security and lawful processing shall always be considered when selecting Company's associates. The Company's associates shall take into account the terms hereof as far as it concerns them regarding the observance of rules of access to the Company's systems, management of security incidents, security measures, etc., in accordance with the nature of the processing they have undertaken.

5.5. Access rights to the Company's IT systems shall be granted exceptionally to personnel members of the Company's associate when this is necessary for the fulfilment of its contractual obligations. In such case, only the minimum necessary authorisations shall be granted, which shall be abolished upon the expiration of the contractual obligation.

6. Technical and organizational measures

6.1. The Company's internal procedures include appropriate technical and organisational measures to ensure an adequate level of security against risks arising from processing, especially those arising from accidental or unlawful or unfair destruction, loss, alteration, unauthorised disclosure or access of Personal Data transferred, stored or otherwise processed. Such measures shall aim, inter alia, at ensuring the ongoing confidentiality, integrity, availability and reliability of the processing systems and services; at restoring availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and at regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2. Company Officers shall only have access to such Personal Data as necessary for the performance of their duties ("need to know basis"), which they process in compliance with the principles of Personal Data processing. The relevant access authorisations and rights shall be reviewed, as necessary, during the course of business or other existing relationship.

6.3. Company Officers shall maintain the confidentiality of the Personal Data that they may process in the course of performing their duties. The physical records of Personal Data shall be diligently kept, e.g. in lockable cabinets, etc.

6.4. Company Officers shall refrain from leaving any documents and portable storage media containing Personal Data unattended in their office ("clean desk policy"). Portable storage media should be kept in safe places when not in use and always supervised while in use.

6.5. Company Officers shall comply with Guideline 1/2005 of the Data Protection Authority regarding safe destruction of personal data after the end of the period required for the purpose of the processing or by other relevant legislation, as well as with the procedures for the destruction of electronic documents and data applied by the Company in case these contain Personal Data and their storage is not required.

6.6. Company Officers should make sure that the exit door is properly closed when they leave

the Company premises. Company Officers are required to safeguard the keys/access cards to the Company's facilities and not to lend them to third parties, and to generally comply with the rules and procedures applied by the Company in relation to the operation of its facilities.

7. Use of Communication means - Equipment

Any machine and equipment, in general, used to facilitate communication at the workplace or in relation to work (such as telephones, fax machines, laptops, desktop computers, etc.) are Company assets, which Company Officers are required to handle diligently in accordance with the Company's instructions and with respect to any Personal Data communicated through them, in compliance with the principles governing the processing of Personal Data.

7.1. The above communication means, including e-mail and internet provided by the Company, etc. ("Communication Means") should be used by the Company Officers solely for business purposes.

By way of exception, the Company may allow Company Officers to also make personal use of corporate mobile phones. If an Officer is required to send a personal e-mail, he/she should use his/her personal (non-corporate) account. Company Officers shall use their corporate account exclusively for the performance of their duties.

7.2. The Company is entitled to have access to Officers' Personal Data transmitted via the Communication Means for the purposes described in the law and in relevant guidelines of the Data Protection Authority, such as protection of persons and goods, organization, and work execution or turnover control, including cost control and, in general, for the satisfaction of the Company's legitimate interests, etc., in accordance with the Company's procedures and the processing principles maintained by the Company.

7.3. The Company keeps backup copies in accordance with its procedures in order to ensure the availability and integrity of Personal Data.

7.4. Company Officers should select very strong passwords to their computer and change them on a regular basis, in accordance with the Company's procedures. Company Officers-users should keep their passwords confidential and not make them accessible to third parties. If they are required to disclose a password to the technical support department for the purpose of resolving a technical issue, they should change it immediately after the technical issue has been resolved. After a certain number of repeated failed login attempts, the authorized user will be denied access.

7.5. Company Officers-users should not change the program settings selected by the Company for data security, such as anti-virus and firewall programs. In the event that users become aware of a virus, or a breach or an attempted breach of Personal Data in general, they must the Company without delay. Spam emails should not be opened but should be immediately deleted by the Company Officers-users.

7.6. Company Officers-users should mark an email as "Confidential" and possibly protect it by password or otherwise, in the event that an e-mail containing confidential or special category information is required to be sent, in accordance with the relevant instructions and procedures of the Company.

7.7. Upon dissolution or termination of the employment or other relationship, Company Officers are required to return any equipment provided by the Company for them to perform their duties and serve the Company's operational needs, and to cease to use it in any case. In

such case, the Company shall immediately remove all access accounts, authorizations and passwords of such user.

8. Rights of data subjects

8.1. The Company and its authorised Officers shall facilitate the exercise of the Data Subjects' rights stipulated by national and EU laws in accordance with the relevant instructions of the Company. Company Officers shall immediately inform the Company of any request regarding the processing of the Data Subjects' Personal that comes to their knowledge. Furthermore, the Company encourages each Data Subject to submit questions to the Company in relation to this Policy.

8.2. The Company shall provide the Data Subject with information on the action taken at his/her request without delay and in any case within the time limits set out by law. If the Data Subject submits his/her request by electronic means, the information shall also be provided, if possible, by electronic means, unless the Data Subject requests otherwise.

8.3. Data Subjects shall not be discriminated against because they have exercised their statutory rights.

8.4. Data Subjects may exercise their envisaged rights by post to the address of the Company's headquarters or by telephone or via e-mail to dpo@hcap.gr.

9. Information & Access

9.1. When Data Subjects provide their Personal Data to the Company, they are informed by the Company about the processing of such Personal Data.

9.2. The information includes all the details stipulated by the law unless they are already known to the Data Subject.

9.3. If the Data Subject so wishes, he/she shall receive confirmation from the Company as to whether the Personal Data concerning him/her are processed and, if so, he/she may have access to them as well as to information on the processing of such Personal Data, as defined by law.

10. Rectification

10.1. The Data Subject may request from the Company the rectification of inaccurate or completion of incomplete Personal Data concerning him/her.

11. Deletion

11.1. The Data Subject may request from the Company the erase Personal Data concerning him/her.

11.2. The Company shall erase the Data Subject's Personal Data, if it is proven that one of the

reasons stipulated by law applies (e.g. the Personal Data are no longer necessary in relation to the purposes for which they were collected; data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing, etc.).

11.3. The Company has the right not to delete Personal Data, if one of the reasons stipulated by law applies (e.g. compliance with a legal obligation which requires processing, establishment, exercise or defence of legal claims, etc.).

12. Restriction of processing

12.1. The Data Subject may request from the Company the restriction of Personal Data processing, if it is proven that one of the reasons stipulated by law applies.

12.2. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

13. Objection

13.1. The Data Subject shall have the right in all cases set out by law to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her.

13.2. The Company shall no longer process the personal data unless there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

14. Data protection officer

14.1. The Company appoints a Data Protection Officer, to whom the Company's Officers/Data Subjects may address any issue or question regarding Personal Data processing and use of the Company's communication means (by telephone or via e-mail to dpo@hcap.gr).

15. Training

15.1. The Company shall ensure that its Officers receive training in relation to Personal Data processing and the implementation of this Policy. Company Officers shall be required to participate in such training.

16. Cooperation with Supervisory Authorities

16.1. The Company and its competent Officers shall cooperate with the Hellenic Data Protection Authority, which is responsible for supervising the implementation of the national legislation on the protection of Personal Data.

17. Completion – Revision

17.1. This Policy is supplemented by procedures and specific instructions, which are based on this Policy and must be applied by Company Officers or third parties, as required. In case of failure to comply with this Policy as well as the relevant procedures and other instructions, the Company shall take all appropriate measures at its discretion, or terminate the employment/cooperation contract, etc., and exercise its legitimate rights against persons who violate them.

17.2. This Policy shall be revised by the Company, as required, especially in the event of an amendment to the legislative framework for Personal Data protection and processing or the security requirements.

Personal Commitment

I hereby certify that I have received a copy of the Company's Policy on Personal Data Protection & Processing and Use of Communication Means, have studied and understood the Policy, and accept and abide by the principles, rules and standards of conduct contained therein as required. I currently have no information about any violation of the Policy.

Date: _____

Full Name: _____

Position: _____

Signature: _____