

## DATA PROTECTION POLICY STATEMENT

HELLAS SAT's (hereinafter the "Company") main priority is the respect and protection of personal data processed in any form. To this end, this Data Protection Policy Statement has been adopted to govern the processing of personal data in HELLAS SAT's operations by its executives and its individual departments and directorates. In addition, We are aware of how important your personal data are to you and we respect that. For this reason, we use your personal data with care, having adapted our data protection policy to the provisions of the General Data Protection Regulation No. 2016/679/EC (hereinafter the "GDPR") which came into effect on 25 May 2018.

We hereby wish to inform you about the types of personal data we collect, the reasons and purposes for which personal data are collected and what we do with personal data. We also wish to inform you about your rights in connection with such processing of your data.

Please dedicate a few minutes to learn about our practices relevant to the processing of personal data; having done so, if you have any remarks, questions or queries please contact us by e-mail or by submitting a request via the Communication form available in our website [www.hellas-sat.net](http://www.hellas-sat.net).

### Basic Definitions and Processing Principles

**Processing** of personal data means any operation or set of operations which is performed, whether or not by automated means, on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The processing of personal data by the Company is governed by the following Principles:

**a) Legitimacy, objectivity and transparency:** Personal data shall be processed lawfully and fairly in a transparent manner in relation to the data subject.

**b) Purpose limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.

**c) Data minimisation:** Personal data shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

**d) Accuracy:** Personal data shall be accurate and, where necessary, kept up to date; all reasonable steps shall be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are erased or rectified promptly.

**e) Limitation of the storage period:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, provided that the personal data will be processed only for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1) of the GDPR and provided that appropriate technical and organisational measures are in place to safeguard the rights and freedoms of the data subject.

**f) Integrity and confidentiality:** Personal data shall be processed in a manner that ensures appropriate security of such data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Accountability:** The Company as the Data Controller is responsible for and able to demonstrate compliance with the above Processing Principles.

### **Who collects my data?**

#### **Greece office:**

The Company « HELLAS SAT SINGLE MEMBER SOCIETE ANONYME SATELLITE SYSTEMS AND COMMUNICATIONS SERVICES », trading name «HELLAS SAT» (hereinafter referred to as the «Company») has its registered office at 48, Konstantinoupoleos Street, Koropi, 19441 District of Attica, Greece.

#### **Cyprus office:**

The Company «HELLAS SAT CONSORTIUM LTD.», trading name «HELLAS SAT» (hereinafter referred to as the «Company») has its registered office at 1, Panagias Galaktotrofousas Street, Kofinou, 7735 Larnaca, Cyprus.



HELLAS SAT is the Data Controller, which means that it determines for what purposes the personal information held, will be used. It is also responsible for notifying the Data Protection Authority of data breaches. The Company was established in August 2001 and is a satellite services provider offering its services in Europe, Middle East and South Africa. In the period 2007-2015 also conducted business activities as a satellite internet services provider. In April 2013 the company Arabsat acquired the majority of the Company shares and since then the Company is a member of Arabsat Group.

This statement covers the collection of personal data by the Company during the development of its business activity, including its presence in websites, platforms and applications of third parties under the Terms of Use of our website.

It is noted that when you visit the Website of our Company, data are collected relevant to your interaction with the website and the installation of cookies (see our Cookie Policy). Third party websites in general apply their own Confidentiality Statements and their own Terms and Conditions. You are urged to read them prior to using the said websites.

### **What are the personal data collected?**

Personal Data means any kind of information relating to an identified or identifiable natural person (the «data subject»). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Due to the nature of the business of our Company, the Personal Data collected by the Company relate mainly to;

- a) employees
- b) prospective employees (during the recruitment and hiring process)
- c) visitors of the Company's premises
- d) partners
- e) customers
- f) website visitors

i.e. their personal data as well as information concerning exclusively their employment relationship with our Company. Employee health data are also collected, in connection with their sick leaves, as well as health data on employees and their dependents for their inclusion in the group insurance policy provided by our Company to its employees.

A small amount of Personal Data is also collected in relation to individual representatives of our active customers, these being legal entities to which we provide satellite service.

For example, the name, role and signature of a signatory to a contract with us, or contact details so we can liaise with the customer.

Further, Personal Data are collected in respect of natural persons entering the Company and its premises.

Finally, the Company keeps a record of non-active customers under the terminated satellite internet services operator business.

### **How are my personal data collected?**

We may collect personal data from various sources, namely:

- Personal data provided to our Company directly by the data subjects, such as details provided by employees and prospective employees, identity details of visitors to our premises, etc., including also health information given upon consent by the employees-data subjects.
- Personal data provided to us directly by our customers.
- Personal data collected from the video surveillance system (CCTV) installed at the entrance/exit of our premises, for the protection of persons, goods and critical infrastructure, with a relevant notice for data subjects in conformance with the applicable legislation.
- Personal data generated in the course of performance of the employment contract of each employee with the Company.
- Personal data collected from the insurance company or the employees, as applicable, in the context of the group policy for the employees and the relevant contractual relationship. It is noted that in this particular processing, the Company is both a Data Controller, in the context that it acts as an employer, and a Processor, in the context that it acts on behalf of the insurance company.
- Personal data collected from the mobile telephony operator that is the business partner of the Company.
- Personal data collected from persons entering the building premises of the Company and from the organizations that such persons represent.
- Personal data collected from (now inactive) customers of the Company in the context of the satellite internet services business.

We also receive and store specific types of personal data each time anyone interacts with us over the internet, i.e. when we use cookies and tracking technologies to obtain personal data and, furthermore, the web browser used by the internet user has access to

our website or our entries, as well as to other content displayed by the Company or for the Company in other websites.

It is pointed out that we do not collect personal data of special categories, other than health data as referred to herein, such as race, ethnic origin, religion, sexual orientation or genetic biometric data etc. which are classified as special data categories and are afforded an enhanced degree of protection in conformance with European data protection legislation.

### **Specifically on the privacy of minors**

Personal data on children may be collected exclusively in the context of the employment relationship with our employees, i.e. for the description of their family status in connection with matters relevant to earnings, labor rights, etc. as well as for the purpose of including minors/dependents in the group insurance policy provided to employees and for serving the said insurance contract. It is understood that such data are provided upon the consent of the person exercising parental responsibility over the child (see also below).

### **For what purpose are my data processed?**

The purpose of processing is commensurate with the specific function being performed; more specifically:

- The personal data of prospective employees, which they themselves provide during the individual candidate selection and evaluation stages (Full name, Address, Contact details, information on education-professional experience, date of birth, identity details, details on social security and tax identification details, family-related data, full name of spouse and details of children) are transmitted to the HR department, the respective hiring Department of the Company and to Management, for the purpose of informing the Company, for the purpose of evaluation and for conducting interviews, etc. for employee hiring and for the conclusion of the relevant cooperation agreement.
- The personal data of employees and business associates, that are provided upon their engagement, upon the conclusion of the employment/cooperation contract with the Company and throughout the term of such contract (in addition to the above, full personal details and details of children, information for the definition of earnings, working hours, details on social security, bank account, etc.), are transmitted to the HR Department for the purpose of the conclusion, performance or termination of the respective employment/cooperation contract.
- Furthermore, upon their engagement, the Company provides to the newly engaged employees information on the provided corporate assets (i.e. corporate mobile phones), accesses to electronic and physical files and work fields for the purpose

of performance of the employment contract. The corresponding data are collected and kept in the Human Resources Department.

- Personal data of employees concerning attendance, absence, hours of attendance, leaves, supporting medical certificates for sick leaves, are kept by the HR Department for the purpose of authorizing leaves, including sick leaves.
- Personal data concerning the performance of employees are provided by the heads of the individual departments also for the purpose of personnel evaluation by the Company.
- Personal health data of employees and their dependents are provided by the employees and by the respective insurance company, to the HR Department for the purpose of the inclusion of employees and their dependents in the group insurance policy provided by the Company as well as for the verification of expenses and payment of compensation to the insured beneficiaries; specifically the financial data (expenses, insurance premiums, compensation money) are provided to the Accounts Office of the Company for processing purposes.
- Personal data of employees concerning the use of corporate mobile phones (numbers dialled, charges), are provided to the HR Department by the respective mobile telephony operator for the purpose of monitoring corporate expenditure and for corporate business organization and handling purposes.
- The Company records the personal details of persons entering and exiting the Company premises (Full name, Identity Card/Passport Number, time of entry/exit), both in respect of its employees and for visitors, for reasons of security and protection of persons (employees) and property/goods (facilities and mechanical equipment). Incoming visitors provide their personal details themselves upon entry, which are matched to the respective personal details already transmitted to the Company by its business partners and similar parties with respect to persons sent by them. The collection of the relevant data is carried out by the building entrance security officer.
- Surveillance of the entrance and the other facilities and the critical infrastructure and mechanical equipment areas is also affected by video cameras in a CCTV system. Every person (employee or visitor) coming into the premises is advised in an appropriate, conspicuous and easy to understand manner (signs) that he/she enters an area which is under closed-circuit television surveillance for reasons of security and protection of persons, goods and critical infrastructure and is also advised of such other information as prescribed by law. Employees, moreover, are additionally advised in writing personally about the said systems and control and surveillance methods and other information as prescribed by law. The methods of control and surveillance and the purpose they serve shall not be an affront to the dignity of employees, they are limited to data directly related to the employment

relationship and do not extend, to the extent possible, to the personal conduct, personal characteristics or personal internal and external contacts of employees. These data are collected and kept, in accordance with the legislation, by the security officer of the building.

- Such processing, i.e. the recording of personal information and the video surveillance of the entrance and the premises, is performed by the Company (as the data processor) also on behalf of a lessee (the data controller), a company operating in a separate space within the same building premises, in fulfilment of a contractual obligation undertaken by the Company as the lessor, vis-a-vis the said lessee, for the security of persons, goods and critical infrastructure. The relevant processing (data collection) is carried out by the security officer of the entrance of the premises. The Company delivers to the lessee only the information that pertains to the lessee.
- Personal data (details of customers, contracts and financial figures) relating to inactive contracts of the Company with customers for the provision of satellite internet services, a business activity terminated in 2015, are kept by IT, the Accounts Office and in physical records, for the purpose of complying with relevant contractual obligations and keeping the necessary tax accounting records.
- We may process any personal data collected by us to comply with, or enter into dialogue relating to, our legal or regulatory obligations; to the extent required to effectively participate in arbitration or litigation; or where required to respond to legal enquiries or to conduct investigations.

### **What is the legal basis of data processing?**

The collection and processing of personal data of the above data subjects is based on:

a) employees: ar. 6 par. 1b GDPR, because the processing is necessary for the performance of the working relationship with our company, but also ar. 6 par. 1c GDPR, because the processing is necessary for compliance with all labor law legal obligations to which our Company is subject;

Employees' data that are used for the group's insurance policy, are collected after the prior consent of the employees', in compliance with ar. 6 par.1a, ar. 6 par.2a GDPR. We must highlight that this extra insurance option is totally optional for our personnel, and it is given only as an option and not as any prerequisite for our contractual obligation;

b) prospective employees: ar. 6 par. 1b GDPR, in order to take steps at the request of prospective employees prior to entering into a contract;

c) visitors of the Company's premises: ar. 6 par.1f GDPR, because the security of natural persons and premises in our Company is a purpose of legitimate interest for our

Company. We respect all personal data principles and fundamental rights and freedoms of data subjects;

d) partners: ar. 6 par. 1b GDPR, because the processing is necessary for the performance of the contractual relationship with our company, but also ar. 6 par. 1c GDPR, because the processing is necessary for compliance with all legal obligations to which our

Company is subject;

e) customers and former customers: ar. 6 par. 1b GDPR, because the processing is necessary for the performance of the contractual relationship with our Company which is based on the one hand on the cooperation contracts with partners and, on the other hand, the -expired- contracts for the provision of satellite internet to customers (an activity which ceased in 2015), but also ar. 6 par. 1c GDPR, because the processing is necessary for compliance with all legal obligations to which our Company is subject;

f) website visitors: ar. 6 par. 1a GDPR, as we obtain the explicit consent of website visitors before installing cookies on their devices, or before the subscribe to our newsletter; and

g) other legal requirements in connection with our legal and tax obligations in general (ar. 6 par. 1c GDPR), or for the purpose of safeguarding our own legitimate interests (ar. 6 par. 1f GDPR) (in the security of persons, goods and infrastructure, in optimizing productivity, to cooperate with law enforcement and regulatory authorities, to engage in litigation or arbitration, or to conduct investigations to protect our interests). We may also rely on necessity for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity, to the extent that processing of special categories of personal data (for example, health data) is necessary for this purpose (ar. 9 par.2f GDPR).

## **Profiling**

The Company does not use personal data for profiling purposes.

## **Transfer of Data to Third Parties: To whom will my data be transmitted?**

The Company in principle does not transmit personal data to third parties, other than in the following cases. More specifically:

- The Company transfers personal data concerning its employees (full name, earnings, date of birth, tax identification number, social security number, annual leaves, home address and employment contract) to the company ARAB SATELLITE COMMUNICATIONS ORGANIZATION (ARABSAT), the majority shareholder of the Company since 2013, for the purpose of integrating IT systems and consolidating financial statements and achieving synergies between associated undertakings. The Recipient has its registered office in a third country



(Riyadh, Saudi Arabia). Data transfer is governed by the Standard Contractual Clauses approved by the European Commission, pursuant to article 46 para. 2 item (c) of the General Data Protection Regulation (GDPR). The said clauses contain adequate and appropriate safeguards on the protection of personal data, as determined by the European Commission pursuant to article 26, para. 4 of Directive 95/46/EC. No Authorization is required for such transfer with respect to the Company's Greek Office. The Company, as the data processor, has advised the Hellenic Data Protection Authority of such transfer. With respect to the (Company's) Cyprus Office the Company has undertaken all actions required by the Cyprus Authorities and applicable legislation which provide for granting of Authorization for such transfer.

- The Company transfers sensitive health data, concerning employees and dependents included in the group insurance policy provided to its employees, to the respective insurance company. The Company also transfers personal data concerning insurance premiums, insurance sums, medical referral certificates, medical reports and other medical documents from/to the insured persons (employees and dependents) to/from the insurance company, in the context of performance of the said insurance contract.
- Where we process any personal data collected by us to comply with, or enter into dialogue relating to, our legal or regulatory obligations; to the extent required to effectively participate in arbitration or litigation; or where required to respond to legal enquiries or to conduct investigations, we may disclose such personal data in connection with proceedings or investigations anywhere in the world to third parties, such as public authorities, the court service, law enforcement agencies, arbitrators, tribunals, regulators and/or third party litigants. These third parties will process your Personal Data for their own purposes and not on our instructions. Unless an alternative export mechanism has been identified, we will rely on Article 49(1)(e) of the GDPR (transfer is necessary for the establishment, exercise or defence of legal claims). We can provide copies of the safeguard relied upon in relation to any specific transfer, on request.
- It is pointed out that the said companies (ARABSAT and the insurance company) have access to personal data that are necessary for them in order to fulfil their specific functions and tasks, but they are prohibited from using them for any other purpose, and moreover they have in advance undertaken binding commitments vis-a-vis our Company with regard to their relevant obligations to not use data for a purpose other than the performance of processing, to observe confidentiality and in general to comply with the Regulation.

- Furthermore, the Company transfers personal data collected at the entrance/exit of its building premises to a lessee operating within the same premises, in fulfilment of a contractual obligation contained in the lease contract between the two companies. The data transferred pertain exclusively to persons coming in the premises of or visiting the said lessee. In this specific personal data processing task, our Company is the data processor on behalf of the lessee who is the data controller.
- For all of our data transfers, we have signed a Data Protection Agreement, according to ar. 28 GDPR, to ensure that our contractual obligations regarding personal data are transparent and committing.

### **For how long are my data stored?**

The data retention period depends primarily on the purpose of processing, given that even the retention of data constitutes an act of processing, which is permitted only if governed by the principles governing data processing. After the lapse of the data retention period, personal data are erased. If personal data is used for two or more purposes, we will retain it until the purpose with the latest period expires; but we will stop using it for the purpose with a shorter period once that period expires. More specifically:

- Personal data of prospective employees are stored in a mail server and a fileserver, accessible to the obligated persons of HR and Management, for a period of one year as of the completion of the selection-recruitment procedure. Such retention serves the purpose of a possible future re-evaluation of candidates by the Company.
- Personal data of employees (and associates), i.e. those parties having entered into an employment/work agreement with the Company, are kept in physical records and in a fileserver by the HR Department in principle for as long as the employment/engagement relationship is in effect. Following the termination of this relationship, howsoever occurring, the relevant data are stored for a maximum period of twenty years, a period during which a legal requirement for the processing thereof may arise, such as for instance in the context of investigation of a criminal offence where an employee may be involved, in case of a tax audit, etc. The above also applies in connection with information on corporate assets provided to employees, on their access to electronic and physical files and work fields and corporate mobile phones, for the purpose of performance of the work relationship; the above also applies with respect to personal data concerning employee leaves (attendance, absence, hours of attendance, leaves, medical certificates in support of sick leaves) and personnel evaluation.
- Personal health data of employees and their dependents are provided to the HR Department by employees and by the insurance company in the context of the

group insurance policy and are kept in physical records, the mail server and the fileserver until the end of the employment relationship. After the termination of the employment relationship, the said data are stored for up to 5 years following the end of the calendar year in which the employment relationship was terminated, unless otherwise directed by the insurance company. Purely financial information on the insurance contract is retained for as long as a tax audit of the respective fiscal years may be conducted.

- Personal data of visitors of our building premises are kept at the Reception until the respective visitors' register is full and are then kept for up to 20 years at the IT – Building Management office. The Company promptly erases from its own records the data of visitors that the Company transfers to another company (lessee) that operates in a separate space within the same building premises as the Company.
- Personal data of employees and visitors from the closed-circuit video surveillance system operating in the building premises, including the entrance and selected work areas, are stored for seven (7) days in a CCTV recorder, subject to specific legislation provisions applicable to specific categories of data controllers. In case of an incident relevant to the purpose of processing, the data controller is permitted to store in a separate file the images in which the specific incident has been recorded, for three (3) months. After the lapse of the said time period, the data controller may store the data for a longer period in exceptional cases only where further investigation into the incident is required. In such a case, the data controller is required to advise the Data Protection Authority about the necessary period during which such images are to be stored.
- Personal data concerning inactive contracts of the Company for the provision of satellite internet services, a business terminated in 2015, are stored by the IT department, the Accounts Office as well as in physical records, for as long as it is possible that a claim may be raised in connection with the fulfilment of the related contractual obligations, i.e. for a period of 5 years after the end of the year in which the respective contractual relationship was terminated, as well as for the purpose of the Company complying with its tax obligations, as prescribed by the tax legislation as applicable from time to time.
- Please note that these periods may be extended where reasonably necessary (for example where we are required to do so by law or by a regulator, for example, "pending trial " or to exercise our legal rights or defend our legal position).

## What is my data protection rights?

The processing of your personal data is associated with rights to which you are entitled in respect thereto which, without prejudice to any law provisions that may limit the exercise thereof, are the following:

- The right to information. You have the right to obtain clear, transparent and intelligible information about how we use your personal data and what your rights are. For this purpose, we provide you with this information in the present Data Protection Policy - Statement and we urge you to contact us for the provision of any clarifications thereon.
- The right to access and rectification. You have at all times the right of access to your personal data and the right to request that your personal data be rectified and updated.
- The right to data portability. The personal data you have provided to us are portable; this means that they can be moved, copied or transmitted by electronic means.
- The right to erasure. Should you at any time withdraw your consent to the processing of your data, you have the right to request that we erase your personal data.
- The right to restriction of processing. You have the right to request the restriction of the processing of your personal data.
- The right to withdraw your consent. If you have given your consent to the processing of your personal data, you have the right to withdraw your consent at any time by contacting us using any of the methods specified herein.
- The right to object is applicable in connection with data processing for direct marketing purposes (e.g. to receive informative email messages from us).
- The right to lodge a complaint with the Data Protection Authority. You have the right to lodge a complaint directly with the local supervisory Data Protection Authority concerning the manner in which we process your personal data. You can contact the Greek Data Protection Authority at [complaints@dpa.gr](mailto:complaints@dpa.gr), or at its premises at Leoforos Kifisias 1-3, 11523, Athens, Greece. You can contact the Office of the Commissioner of Data Protection in Cyprus, at [commissionerdataprotection.gov.cy](mailto:commissionerdataprotection.gov.cy), or at its premises at Iasonos 1, 1082 Nicosia, Cyprus.
- Rights relevant to automated decision-making. You have the right to be excluded from decision-making which is based solely on automated processing and which

has legal or other significant consequences for you. More specifically, you have the right:

- o to obtain human intervention;
- o to express your point of view;
- o to request explanations with respect to a decision that is the result of an evaluation, and
- o to contest this decision.

In case you exercise any of your above rights, we shall take all steps possible in order to satisfy your request within a reasonable time period and at the latest within one (1) month as of the identification of your request, advising you in writing about the satisfaction of your request or about the reasons, if any, that prevent the exercise of the relevant right on your part and/or the satisfaction of one and/or more of your rights, under the General Data Protection Regulation. It is pointed out that in certain cases the satisfaction of your relevant requests may not be possible, such as for instance when the satisfaction of the right contravenes an obligation under the law or runs contrary to the contractual legal basis for the processing of your data.

If, however, you consider that any of your rights or a legal obligation of our Company in connection with Personal Data Protection is infringed, you may lodge a complaint with the competent supervisory authority, namely the Hellenic Data Protection Authority (HDDPA) at the following link: [www.dpa.gr](http://www.dpa.gr). It would, however, be more beneficial for our relationship with you and for our own improvement if we were given the opportunity to hear your concerns directly from you and to address them; we therefore request that, prior to proceeding with any action with the Authority, you communicate first with us, at the contact details provided below.

### **How are my personal data protected?**

We have implemented appropriate organizational and technical measures to protect your personal data against abuse, interference, loss, unauthorized access, alteration or disclosure. Such measures include appropriate measures for access control, technical security of information as well as ensuring that personal data are encrypted, pseudonymized and anonymized, where this is necessary and feasible.

Access to your personal data is permitted only to competent employees and associates of our Company and only if necessary, for supporting the business of our Company, and such access is subject to strict confidentiality contractual obligations when processing is delegated to and performed by third parties.

The obligated persons must immediately inform the Company's Management in case they become aware of any case of infringement or endangerment of the rights of the personal data subjects, intentional or not, due, indicatively, due to an artificial or human factor, an accidental event or force majeure, in order for the Company to take appropriate measures to limit or prevent the infringement and any other legal measure.

### **How can I contact HELLAS SAT?**

#### **Greek office:**

You may contact us at our registered address, at 48 Konstantinoupoleos Street, Koropi, Attica, Postal Code 19441, or at the e-mail address [info@hellas-sat.net](mailto:info@hellas-sat.net) or submit a request using the form available in our website.

#### **Cyprus office:**

You may contact us at our registered address, at Panagias Galaktotrofousas 1, Kofinou, 7735, Larnaca, Cyprus, P.O. box 27556 or at the e-mail address [info@hellas-sat.net](mailto:info@hellas-sat.net) or submit a request using the form available in our website.

### **Update of the present Data Protection Policy Statement**

This statement shall be revised as necessary in order to adapt to legislative changes, to address the views and needs of data subjects and to respond to changes in products, services and internal procedures of the Company. All changes shall be published together with a revision of the date of the latest update shown at the top of the header of each page of this Data Protection Policy Statement.