UNOFFICIAL TRANSLATION

GOVERNMENT GAZETTE
OF THE HELLENIC REPUBLIC

SECOND ISSUE

Edition 2715

November 17, 2011

DECISIONS
No. 165/2011

Regulation for the Assurance of Confidentiality in Electronic Communications

THE HELLENIC AUTHORITY
FOR COMMUNICATION SECURITY AND PRIVACY (ADAE)
(Meeting of 9.11.2011)

Having regard to:

1. The provisions of:

a. article 1(1) and article 6(1) of L. 3115/2003 "The Hellenic Authority for Communication Security and Privacy" (GG A'47/2003);
b. article 5 of L. 3674/2008 "Reinforcement of the institutional framework for the assurance of confidentiality in telephone communications and other provisions" (GG A'136/2008);
c. decision No. 629a/2004 of ADAE "Regulation for the assurance of confidentiality in mobile telecommunications services" (GG 87/2005);
d. decision No. 630a/2004 of ADAE "Regulation for the assurance of confidentiality in fixed telecommunications services."(GG B' 87/2005);
e. decision No. 631a/2005 of ADAE "Regulation for the assurance of confidentiality in telecommunications services via wireless networks" (GG B' 87/2005);
f. decision No. 632a/2005 of ADAE "Regulation for the assurance of confidentiality in internet communications and related services and applications" (GG B' 88/2005);
g. decision No. 633a/2005 of ADAE "Regulation for the assurance of confidentiality in internet infrastructures" (GG B'88/2005);
h. decision No. 634a/2005 of ADAE "Regulation for the assurance of applications and internet user confidentiality" (GG B' 88/2005);
i. decision No. 2654/27.11.2008 of ADAE entitled: "Establishment of a working group for the revision of ADAE Regulations for the assurance of communications

confidentiality contained in Decisions No. 629a, 630a, 631a" (Special Officials and Management Positions of Public Sector and Wider Public Sector Bodies Issue of the Government Gazette No. 510/10.12.2008);
j. decision No. 2660/27.11.2008 of ADAE entitled: "Establishment of a working group for the revision of ADAE Regulations for the Assurance of Communications Confidentiality contained in Decisions No. 632a, 633a, 634a (Special Officials and Management Positions of Public Sector and Wider Public Sector Bodies Issue of the Government Gazette No. 510/10.12.2008).

2. The need to revise the above Decisions of ADAE in order to adopt a single set of Regulation for the Assurance of Communications Confidentiality.

3. The meeting minutes of the plenary session of ADAE at 14.9.2011, 21.9.2011, 28.9.2011, 26.10.2011, 9.11.2011.

4. The fact that this decision does not entail any expenditure for the current or subsequent financial years for the State Budget, we hereby decide:

To issue this Regulation, whose provisions are as follows:

Article 1

Scope

1.1. The provisions of this Regulation concern all persons involved in providing electronic communications networks and/or services. These persons are obliged to have and to implement a Security Policy for the Assurance of Communications Confidentiality whose content must be in accordance with the provisions of this Regulation.

1.2. Persons who provide electronic communications networks and/or services operating under a General Authorisation regime, as it is defined in the legislation in force, are obliged to submit to ADAE for approval the Security Policy for the Assurance of Communications Confidentiality referred to in the previous paragraph, as well as all its revisions whenever they are made. Persons providing the following categories of electronic communications networks and/or services, as stated in the General Licenses Regulation issued by the Hellenic Telecommunications and Post Commission, are exempted from the obligation to submit the Security Policy for the Assurance of Communications Confidentiality to ADAE for approval:

a) A0102: Fixed telemetry, telematics and radio location networks;
b) A0108: Networks for transmitting ground digital broadcasting signals, using frequencies for transmitting radio television signals;
c) A0109: Networks for transmitting ground analog broadcasting signals, using frequencies for transmitting radio television signals;
d) A0204: Private mobile radio network (excluding taxis);
e) A0205: Private mobile radio network (for taxis);
f) A0206: Mobile telemetry, telematics and radio location networks;
g) A0402: Network of satellite news gathering stations (SNG);

h) A0403: Network of earth news gathering stations (ENG);
i) B0204: Telemetry - telematic - radio location service provision;
j) B0205: Location service for ship in distress;
k) B0301: Unidirectional news transmission (sound, image and/or text);
l) B08: Technical provision of broadcasting (B0801 to B0105 inclusive).

Article 2

Definitions

For the purposes of this Regulation, the terms below have the following meanings:

"Communications Data": the content and the related traffic and location data for each communication;

"Security Incident": any incident which may be related to the assurance of communications confidentiality or any special risk of violation of communications confidentiality and all other cases of non-application or special risk of non-application of the Security Policy for the Assurance of Communications Confidentiality;

"Information and Communication Systems (ICS)": systems or terminals of bound provider's on which data communication operations are performed, such as the collection, input, organisation, retention or storage, modification of data, export, use, transmission, dissemination of data or any other form of dispatch, correlation or combining, interfacing, locking, deletion or destruction of communications data. As a minimum, transmission and interface media, switches, routers, management and supervision systems, email servers, firewalls, intrusion detection/prevention systems, malware detection systems, logging systems, subscriber billing systems, customer service and sales systems, telecom fraud prevention systems, databases retaining communications data and applications that access communications data are mentioned;

"Bound Providers (Providers)": persons involved in providing electronic communications networks and/or services hereof.

In any case, the provisions of article 2 of L.3471/2006 ("Protection of personal data and privacy in the electronic communications sector and amendment thereof of L.2472/1999", GG A'133/28.06.2006), as in force shall apply.

Article 3

Security Policy for the Assurance of Communications Confidentiality

3.1. Purpose - Scope of Policy

3.1.1. The Security Policy for the Assurance of Communications Confidentiality aims to protect communications data and ICS from possible risks so as to safeguard the confidentiality of communications.
3.1.2. The Security Policy for the Assurance of Communications Confidentiality relates to users, subscribers, employees and associates of the bound provider.

3.2. General Requirements

3.2.1. The Security Policy for the Assurance of Communications Confidentiality is modular in structure and consists of individual policies which define the security requirements to be met for each individual category of specific topics. The Security Policy for the Assurance of Communications Confidentiality as a minimum includes the individual policies referred to in detail in articles 3 up to 13 of this Regulation.
3.2.2. Where the Security Policy for the Assurance of Communications Confidentiality is integrated and included in a broader information and communication security policy of the provider, the provider must have a file containing a detailed mapping of the way the structure of the information and communication security policy corresponds to the requirements of this Regulation. Providers referred to in article 1 paragraph 2 of this Regulation, are obliged to submit to ADAE the file which contains broad information and communication security policy.
3.2.3. Any failure to comply with the requirements laid down in this Regulation on the Security Policy for the Assurance of Communications Confidentiality, including the individual policies and procedures which implement them, which, indicatively, may be due to the inapplicability or technical inability to cover specific requirements is recorded and adequately documented. The providers referred to in article 1 paragraph 2 of this Regulation shall put in place and implement an internal procedure for recording and documenting the weaknesses referred to in this paragraph.
3.2.4. For the implementation of individual policies, specific security procedures and organisational structures are defined, documented, implemented and revised. The security procedures define specific actions to be taken by employees, associates, users and subscribers of the provider, the sequence of such actions, the persons responsible for implementing them and the documentation method and means.
3.2.5. The Security Policy for the Assurance of Communications Confidentiality with the individual policies that compose it, defines the management entities or natural persons with specific responsibilities for implementing the policy. The providers appoint the persons responsible for laying down and implementing the design, development, procurement, installation, operation, management, maintenance, upgrade, update, deletion, withdrawal and access rules for each ICS.
3.2.6. The provider is obliged to appoint a specific employee as the Communications Confidentiality Assurance Officer charged with the responsibility of control of the implementation of the measures and requirements laid down in the Security Policy for the

Assurance of Communications Confidentiality. The providers referred to in article 1 paragraph 2 of this Regulation are obliged to inform ADAE of the contact details of each Communications Confidentiality Assurance Officer.

3.2.7. The Security Policy for the Assurance of Communications Confidentiality defines specific stages to be used and implemented in managing the policy. The stages referred to in this paragraph include the identification and risk assessment, design and implementation of security measures and checking implementation thereof.

3.2.8. According to articles 3 up to 13 of this Regulation, it is required to maintain files for the purpose of monitoring the Policy for the Assurance of Communications Confidentiality. Subject to the provisions of L.3471/2006 (GG A'133), L.3783/2009 (GG A'136) and L. 3917/2011 (GG A'22), as in force, the provider is obliged to maintain the files in question for a period of 2 years, taking the appropriate measures to safeguard their integrity, confidentiality and availability. Where an audit is being carried out by ADAE, the provider is required to maintain the files in question even after the end of the 2-year period and to delete them only when a decision of ADAE on that matter has been taken.

3.2.9. Regarding the log files in articles 6.2.5 and 8.3.3.2 of this Regulation, the provider is required to ensure that the records specified in those articles are complete and continuous. The provider is obliged to maintain a Special Log File Template, which as a minimum, include the architecture and individual methods for generating, collecting, storing and managing the log files, a full description of the content thereof, and the measures required to safeguard their integrity, confidentiality and availability.

The provider is obliged to implement the Security Incident Management Policy in accordance with article 9 of this Regulation, where the logs referred to in the above-mentioned articles are interrupted and in the case of a violation of their integrity, confidentiality and availability.

3.3. Information Risk Assessment Procedure

3.3.1. The provider is obliged to maintain and implement an Information Risk Assessment Procedure relating to the confidentiality of communications based on a risk assessment methodology that takes into account international practices. The Information Risk Assessment is carried out at least every 2 years and includes at least the following:

3.3.1.1. Retention of the ICS Catalogue with a brief description of its function.

3.3.1.2. Assessment of threats associated with a possible communications confidentiality violation by external threats, employees or associates of the provider, assessment of ICS vulnerabilities and assessment of possible impacts of communications confidentiality violation incidents.

3.3.1.3. The risk assessment results are taken into account in preparing and revising the Security Policy for the Assurance of Communications Confidentiality and in implementing appropriate measures to give effect to that Policy. The risk assessment results are maintained by the provider and are available during scheduled or unscheduled audits carried out by ADAE into the implementation of the Security Policy for the Assurance of Communications Confidentiality.

Article 4

Acceptable Use Policy

4.1. Purpose - Scope of Policy

The Acceptable Use Policy defines the obligations of the provider and the principles, rules and consequences for employees and associates, to whom access rights to ICS and communications data are granted and aims to prevent abusive exercise of those rights and acts which violate or constitute a risk of violation of the communications confidentiality of subscribers or users of the networks or services provided.

4.2. General Requirements - Obligations
4.2.1. Employees and associates of the provider are obliged to comply with the Security Policy for the Assurance of Communications Confidentiality including the relevant procedures, security measures and guidelines. To that end, the provider is obliged to record the Acceptable Use Policy in a manner which ensures that employees and associates are made aware of it and have accepted the Security Policy for the Assurance of Communications Confidentiality in relation to the work they perform before acquiring access to the ICS and communications data.
4.2.2. The provider is obliged to inform using any reasonable means and train employees and associates regarding the implementation for the Assurance of Communications Confidentiality Security Policy and its amendments.
4.2.3. The employees and associates of provider, who acquire access to ICS and communications data of subscribers or users of the networks or services provided, shall not be permitted to disclose any information or data which comes to their attention or into their possession as a result of the nature of the work they perform.
4.2.4. The employees and associates of the provider shall be obliged to immediately inform the responsible personnel in the case where they become aware of a security gap or related incident which puts at risk the confidentiality of communications of subscribers or users of the networks or services provided.

4.3. Additional Requirements for Associates

4.3.1. The provider is obliged to keep an updated file of associate records, whether natural persons or legal entities, who acquire or may acquire access to the communications data of subscribers or users of the networks or services provided, for the purpose of providing their services.
4.3.2. The provider is obliged to sign contracts with the associates referred to in the previous paragraph, whose minimum content shall be as follows:
4.3.2.1. Terms regarding non-disclosure and confidentiality compliance.
4.3.2.2. Requirements and security measures taken for the assurance of communications confidentiality which safeguard the confidentiality and integrity of communications data when it is being processed by the provider's associates and the final deletion and destruction thereof after the termination of the collaboration.
4.3.2.3. Acceptance by the provider's associates of the need to comply with security measures for the assurance of communications confidentiality referred to in paragraph 4.3.2.2 of this article.

4.3.3. The provider is obliged to activate the Security Incident Management Policy in accordance with article 9 of this Regulation for each violation of the contractual terms set out in paragraphs 4.3.2.1, 4.3.2.2 and 4.3.2.3 of this article.

4.4. Additional Requirements for Subscribers or Users of Networks or Services Provided.

The provider is obliged to inform subscribers or users of networks or services provided, at least during when the contract is being signed with them, and at regular intervals thereafter, using all reasonable means, about the appropriate measures they should be taking to protect communications confidentiality, particularly in relation to proper usage rules of networks or services provided and the methods of using information security technologies and resources associated with the assurance of communications confidentiality.

4.5. Management of Storage Media

The provider is obliged to define in the Policy and implement measures and/or procedures relating to the use, dispatch and destruction of storage media, whether in electronic or hardcopy format, which contain communications data or other information which could lead to the disclosure of communications data of subscribers or users of the networks or services provided (indicative such as access codes and ICS structural data) so as to prevent them from being disclosed to non-authorised persons.

Article 5

Physical Security Policy

5.1. Purpose - Scope of Policy

The Physical Security Policy defines the measures required to prevent unauthorised physical access to the provider's facilities where the ICS are installed, apart from those used exclusively to serve the public, and shall also cover the access control to those facilities and the ICS protection.

5.2. General Requirements

5.2.1. The provider is obliged to take all necessary and adequate measures to physically protect its facilities, so as to prevent all unauthorised access to them and to control physical access so that access is only permitted to authorised persons.
5.2.2. The provider is obliged to draw up and implement a physical access procedure which sets out in detail all required measures for granting access to the facilities and spaces within his premises to the employees and associates where ICS are installed.
5.2.3. In order to grant physical access authorisation to employees or associates of the provider to facilities and spaces within the premises where ICS are installed, prior authorisation by the competent management entity or competent natural person shall be mandatory. The provider is obliged to keep a record logging all approved physical accesses, where all data related to each authorisation are recorded (i.e. timeframe, facility or location with access rights.).

5.2.4. Physical access by authorised persons to the provider's facilities shall be logged (i.e. name/surname, position, entry and exit time) in the relevant file. In case the facilities are accessed by an associate of the provider or another visitor, the file referred to within this paragraph must also record the access reason and the details of the employee (name/surname and position) that this person is to meet.
5.2.5. The provider is obliged to designate secure areas within its facilities where ICS are installed. These areas must be protected by robust security mechanisms (i.e. direct detection systems for unauthorised access and CCTV) and controlled access systems (i.e. controlled entry cards) in compliance with the relevant legislation. Physical access to the areas referred to within this paragraph shall be logged in accordance with the requirements of paragraph 5.2.4 of this article. In case associates of the provider or visitors access the areas referred to within this paragraph, they must be accompanied by an authorised employee throughout the duration of their presence. The areas referred to within this paragraph as well as the security and controlled access mechanisms must be logged in a file.
5.2.6. The provider is obliged to take all necessary physical protection and controlled access measures to protect the ICS under its supervision that are installed outside its premises. The security mechanisms for these cases must be described in a file.

Article 6

Logical Access Policy

6.1. Purpose - Scope of Policy

6.1.1. The Logical Access Policy defines the classification of access levels and sets the requirements for access control to the provider's ICS.
6.1.2. The Logical Access Policy should apply to the provider's employees and associates who as part of their work acquire access to the ICS and the relevant data and information.

6.2. General Requirements

6.2.1. Suitable access control mechanisms and provider employee and associate authentication mechanisms shall be used in order to acquire access to an ICS. As a minimum, access control and authentication shall be achieved by using an account comprised of a username and password or other mechanism which ensures an equivalent security level. The provider is obliged to retain a file setting out in detail the access control and authentication mechanisms for each ICS.
6.2.2. Each employee and associate of the provider shall be granted an account for each ICS so that it is possible to match the corresponding person to actions performed on each ICS. The provider is obliged to retain a file mapping the accounts to employees and associates so that it is possible to confirm who uses each account and for what time period.
6.2.3. The creation of group and/or predefined accounts should be avoided. Where that is not feasible, it must be justified and in all events the provider must ensure that persons who acquire access to the ICS can be matched to actions performed on the ICS, using another suitable mechanism which is documented in a file which the provider is obliged to retain.
6.2.4. The provider is obliged to retain a file comprising of access profiles and access privileges for each ICS.

6.2.5. The provider is obliged to retain a log file of user's access to ICS, logging as a minimum the username, the date and start and end time of each access.
6.2.6. Provider is obliged to record in a file the methods by which employees and associates have accessed the communications data of subscribers or users of the networks or services provided. Any access to the communications data of subscribers or users of the networks or services provided must be logged and justified.

6.3. General Logical Access Policy Procedures

Provider is obliged to develop and implement the procedures set out below:
6.3.1. ICS User Management Procedure
6.3.1.1. The ICS User Management Procedure must clearly describe the way in which new ICS users are added, ICS users are deleted and how access profiles or privileges are assigned or changed.
6.3.1.2. For each action referred to in paragraph 6.3.1.1 hereof, prior approval by the competent employee of the provider should be required.
6.3.1.3. The ICS User Management Procedure must set the obligation of retaining the user applications for all changes regarding their access to ICS.
6.3.1.4. The ICS User Management Procedure must set the obligation of maintaining a file with all accounts which have been approved for access to ICS (including the access profiles and types and the time period that each account was active).
6.3.2. Logical Access Policy Proper Implementation Audit Procedure
6.3.2.1. The Logical Access Policy Proper Implementation Audit Procedure must clearly describe the periodic audits carried out in line with the principles of the Audit Policy for the implementation of the Security Policy for the Assurance of Communications Confidentiality referred to in article 11 of this Regulation in relation to:

(a) audits of access types of ICS users, namely whether the access type of each user is the one that actually assigned to the user;
(b) audits of accounts, namely the comparison of the approved applications (para. 6.3.1.4 of this article) with the accounts for each ICS;
(c) audits of the access logs to identify any possible unjustified access.

6.4. Access Account Creation and Management

6.4.1. When creating and managing access accounts, the provider is obliged to retain the following information (per ICS or overall):

(a) a file describing the rules under which a username is created;
(b) a file describing the rules under which a password is created;
(c) a procedure for securely delivering to all employees and associates of the provider the usernames and passwords relating to them;
(d) a procedure for regular changes and management of passwords;
(e) a file describing the terms of use of passwords by the provider's employees and associates;
(f) a procedure for carrying out audits on proper implementation of the said rules and procedures in line with the principles of the Audit Policy for the implementation of the

Security Policy for the Assurance of Communications Confidentiality referred to in article 11 of this Regulation.

6.4.2. In order to implement the obligations of paragraph 6.4.1 hereof, the provider is obliged to take into account the following requirements:
6.4.2.1. The usernames must not include the role of the provider's employees and associates in the ICS (indicative they must not be derivatives of the word 'admin').
6.4.2.2. The passwords used must be strong and have been created in a way to prevent them being hacked easily. In particular, passwords must be created with a combination of at least 2 different types of characters (numbers, letters, and special characters). Passwords must necessarily be of a sufficient minimum length, the use of recent old passwords must be prohibited and specific patterns should not be followed when creating the codes.
6.4.2.3. Passwords must be changed periodically at a frequency set specifically for each ICS and stated in a file which the provider is obliged to retain. The provider is obliged to use and record in that file the ways in which enforce the periodic change of passwords. Cases such as deletion of an ICS user or violation of an account must require an immediate change of passwords.
6.4.2.4. Where a false password is repeatedly keyed in (for example three consecutive failed attempts) the password must be deactivated or it can only be used after the elapse of a specific time period.

6.5. Special Requirements for Subscribers or Users of Networks or Services provided

6.5.1. The provider is obliged to retain a file recording in detail the access control and authentication mechanisms used for their subscribers or users access to the networks or services provided.
6.5.2. The provider is obliged to put in place and implement a specific procedure for managing the accounts of subscribers or users of the networks or services provided clearly setting out as a minimum the method for adding and deleting accounts and the assignment of user names and passwords to subscribers or users of the networks or services provided.
When creating or re-issuing passwords, the provider is obliged to create them in a way that they are prevented from being easily hacked. The provider is also obliged to inform subscribers or users of the networks or services provided using all reasonable means about the necessity to change their passwords and the recommended rules for creating strong passwords.
6.5.3. The provider is obliged to have a procedure in place for carrying out periodic audits relating to changes of passwords assigned to subscribers or users of the networks or services provided and ensure that he is informed about the necessity to change their passwords if they have not made the relevant changes, in line with the Audit Policy for the implementation of the Security Policy for the Assurance of Communications Confidentiality referred to in article 11 of this Regulation.
6.5.4. Where the provider offers to subscribers or users of the networks or services provided the option to acquire access to their communications data (such as outgoing calls, email) via a specific website, it is obliged to use widely accepted secure authentication and encryption mechanisms and describe those in a file that is obliged to retain.
6.5.5. The provider is obliged to inform subscribers or users of the networks or services provided, at least when the contract is signed between them, in hardcopy or in electronic format and at an easily accessible location on its website about the recommended rules for protecting their passwords. Those rules must take into account widely accepted international practices.

Article 7

Remote Logical Access Policy

7.1. Purpose - Scope of Policy

7.1.1. The Remote Logical Access Policy defines the access levels and sets the requirements for controlling the remote access to the provider's ICS.
7.1.2. The Remote Logical Access Policy shall apply to the provider's employees and associates who as part of their work acquire remote access to the ICS and the relevant data and information.

7.2. Remote Access by Provider's Employees and Associates

7.2.1. Remote access by provider's employees and associates to the ICS shall be limited to cases where that is necessary for its operational needs.
7.2.2. Providers shall register in a file the ICS to which remote access is allowed, and the technical methods for granting remote access to employees and associates for each ICS for which remote access has been allowed.
7.2.3. A file shall be maintained with the employees and associates (name/surname and position) of the provider who have been granted remote access rights. This file must record the access rights corresponding to each ICS.
7.2.4. Remote access by the provider's employees and associates shall be performed using secure authentication and encryption mechanisms (such as VPNs).
7.2.5. The provider shall ensure that each connection by employees and associates interfacing its ICS is only permitted to cases where this connection does not violate any of the security rules for its network.
7.2.6. Remote access by the provider's employees and associates shall only be permitted for a specific time frame and shall be performed using temporary codes that will be modified after the end of the specific time frame or by deactivating accounts after the end of that time frame.
7.2.7. The provider shall bind remote access to their employees and associates following approval of the relevant requests which shall designate the access reason, the system to be accessed and the required time period. The provider shall keep a file recording all the information required by this paragraph.

7.3. Remote Access Account Management Procedure

7.3.1. The provider shall put in place and follow a specific procedure managing the remote access accounts of their employees and associates which shall be in accordance with the requirements set out in paragraph 7.2 of this article.
7.3.2. The provider shall check at least every 3 months (a) the consistency between the remote access accounts and the file referred to in paragraph 7.2.3 of this article and b) the implementation of the necessary passwords modification and accounts deactivation referred to in paragraph 7.2.6 of this article, in compliance with the principles set out in the Audit Plan of the Security Policy for the Assurance of Communications Confidentiality referred to in article 11 of this Regulation.

Article 8

ICS Management and Installation Policy

8.1. Purpose - Scope of Policy

The purpose of the ICS Management and Installation Policy is to identify the requirements which must be met during the design, development, procurement, installation, operation, management, maintenance, upgrading, updating, deletion, withdrawal of ICS in order to protect the confidentiality of communications.

8.2. General Requirements

8.2.1. During management and installation of ICS, the provider must take all necessary measures to minimise the risk of information leakage related to the confidentiality of the communications of subscribers or users of the networks or services provided.
8.2.2. Changes (input/modification/deletion) to the ICS software/hardware associated with the assurance of communications confidentiality must be carried out without undue delay.
8.2.3. In the case of any modification in ICS hardware or software, the provider is obliged to retain a file recording the date, manner, reason and employee or associate who performed the modifications. The file shall be updated and retained by a specific management entity or employee of the provider.

8.3. ICS Management and Installation Procedures

The provider is obliged, as a minimum, to maintain and implement procedures relating to the following stages:

i. procurement – development of hardware and software;
ii. installation and commissioning of hardware and software;
iii. maintenance - support - commissioning of hardware and software;
iv. deletion – withdrawal of hardware and software.

8.3.1. ICS Hardware / Software Procurement – Development Procedure
8.3.1.1. The provider shall assess the risk to identify possible threats, weaknesses and risks associated with the confidentiality of communications in the ICS to be procured / developed, in line with the provisions of paragraph 3.3 ‘Information Risk Assessment Procedure’ of this Regulation.
8.3.1.2. In the framework of the ICS Hardware/Software Procurement – Development Procedure, the provider shall prepare a list of requirements relating to settings or specifications of the ICS to be procured/ developed regarding the assurance of communications confidentiality. The communications confidentiality assurance requirements shall also include the minimum requirements relating to the configuration and management characteristics of the ICS to be procured / developed and the configuration requirements for logging user access and user commands, so as to comply with the security requirements specified by the results of the risk assessment and by the best security practices. The files referred to in this paragraph shall be approved by the competent staff of the provider and retained.

8.3.2. ICS Hardware / Software Testing, Acceptance and Proper Operation Verification Procedure
8.3.2.1. Tests shall be carried out regarding the deployment or configuration of the requirements laid down in the Communications Confidentiality Assurance requirements development stage and compliance with those requirements shall be checked. The results of tests shall be recorded and held in a relevant file.
8.3.2.2. After successful completion of the operational testing, an acceptance report for the ICS shall be prepared and signed by the stakeholders who shall be held by the provider in a relevant file.
8.3.2.3. During the initial deployment phase, the proper operation of the ICS shall be monitored so as to timely identify vulnerabilities or security breaches. The results of checks shall be recorded and held in a relevant file.
8.3.3. ICS Hardware / Software Maintenance – Support – Commissioning Procedure
8.3.3.1. The minimum requirements of the ICS Hardware / Software Maintenance – Support – Commissioning Procedure include monitoring of the proper operation of the ICS, by checking incidents and alarms on each system to promptly identify and vulnerabilities or security flaws.
8.3.3.2. The provider shall be obliged to record and retain in a respective file events and user actions on the ICS operating system and applications events as well as the ICS system incidents.
8.3.4. ICS Hardware / Software Deletion - Withdrawal Procedure
8.3.4.1. The provider is obliged to specify particular actions to ensure that, subject to compliance with the obligations deriving from other provisions of the relevant legislation, when ICS hardware or software is deleted or withdrawn, the information stored on the ICS hardware (such as ROM memories, hard disks, magnetic tapes, etc.) is deleted once and for all and cannot be retrieved or used by third parties.
8.3.4.2. The provider is obliged to retain a file recording the ICS which have been withdrawn.
8.3.4.3. The provider is obliged to retain a file recording the actions taken to delete ICS data which must as a minimum record the username of the employee or associate who performed the deletion.

Article 9

Security Incident Management Policy

9.1. Purpose - Scope of Policy

The purpose of the Security Incident Management Policy is to (a) record the details about all security incidents, (b) investigate the causes and identify the technical and/or organisational weaknesses to which the security incident is due, (c) specify the consequences and implement the recovery actions within a specific timeframe, depending on the case and (d) inform:

i. the Communications Confidentiality Assurance Officer and the competent executives of the provider;
ii. the competent Authorities; and
iii. the affected subscribers or users of the networks or services provided, in accordance with the relevant legislation.

9.2. General Requirements

9.2.1. The provider is obliged to define and implement a Security Incident Management Policy, which will be promptly activated in case of a security incident.
9.2.2. The Security Incident Management Policy anticipates that all data referred to in paragraph 9.1 of this article are recorded, and that all records related to a security incident are compiled and retained in a file, which documents that the relevant actions specified have been followed.
The following information is as a minimum recorded:

a. date, occurrence time and description of the incident;
b. data and time at which the provider became aware of the incident;
c. location at which the incident occurred (i.e. system, service, application, protocol, data type);
d. estimated cause of the incident occurrence;
e. consequences of the incident (i.e. number of users affected, type and volume of data);
f. data collected by the provider to investigate the incident (such as log files, data about the violation etc.);
g. information about possible multiple occurrences of the incident;
h. problem resolve time;
i. corrective measures and the relevant timeframe;
j. information provided to subscribers or other persons affected by the incident, and notification of competent authorities in accordance with the relevant legislation;
k. possible recommendations to subscribers or other persons affected by the incident in order to moderate the negative impacts of the incident.

9.2.3. In the case of a security incident, the providers referred to in article 1(2) of this Regulation are obliged to promptly inform ADAE, by submitting a document entitled ”Direct Report of Security Incident” for each incident. The “Direct Report of Security Incident” records as a minimum the information specified in paragraph 9.2.2 of this article, according to the data available at the time of the briefing. After the incident has been addressed and investigated, the providers, referred to in this paragraph, submit to ADAE a document entitled “Security Incident Final Report”, setting out in detail all the information referred to in paragraph 9.2.2 of this article and all additional information, which the provider may have at its disposal.
9.2.4. The Security Incident Management Policy defines the competent executives of the provider, to whom the security incidents must be immediately reported, as well as their relative contact details.
9.2.5. The provider is obliged to enable their subscribers or users of their networks or services to notify possible violations of their communications confidentiality using simple means (e.g. via their website).
9.2.6. The provider is obliged to check at regular intervals the activation readiness of the Security Incident Management Procedure, in accordance with the principles of the Implementation Audit Policy of the Security Policy for the Assurance of Communications Confidentiality, referred to in article 11 of this Regulation.

Article 10

Network Security Policy

10.1. Purpose - Scope of Policy

The purpose of the Network Security Policy is to ensure logical partitioning of the provider's networks from external networks and to segment its networks into security zones or sub-networks, depending on the security level required, in order to isolate ICS in security zones, to partition them at network level and to control data exchange between them.

10.2. General Principles for Network Security Policy Mechanisms and Systems

10.2.1. The provider is obliged to prepare and retain a constantly updated file setting out the hardware and software mechanisms and systems used for the purposes of Network Security Policy, along with their operational and technical configuration, which must take into account international, widely accepted practices and standards, as well as the risk assessment performed by the provider in accordance with the principles set out in paragraph 3.3 of this Regulation. The Network Security Policy mechanisms and systems may include but are not limited to firewalls, IDS/IPS, access control lists, VPNs, VLANs.
10.2.2. Installation, updating and management of the mechanisms and systems referred to in paragraph 10.2.1 of this article must be done in accordance with the ICS Management and Installation principles referred to in article 8 of this Regulation, including the access or control rules configured within these mechanisms and systems (e.g. updates to the IDS/IPS with new attack / intrusion signatures).
10.2.3. The mechanisms and systems referred to in paragraph 10.2.1 of this article must be operated on a continuous basis with the exception of cases of scheduled maintenance or upgrades, in accordance with the ICS management and installation principles referred to in article 8 of this Regulation.
10.2.4. Where a mechanism or system referred to in paragraph 10.2.1 of this article identifies an unusual incident, an alert shall be activated indicating the type, nature and criticality of the incident, while all available information about it shall be logged and retained in a specialised file for further processing. Depending on the criticality of the incident, the provider shall activate the Security Incident Management Policy in accordance with article 9 of this Regulation.

10.3. Logical Partitioning and Segmentation of the Provider's Networks

10.3.1. The provider is obliged to prepare and retain a constantly updated file that, based on the mechanisms and systems of paragraph 10.2.1 of this article, sets out in detail the logical partitioning and segmentation of networks, accompanied by an applicable network diagram, describes the architecture which has been adopted, and records all ICS and the security zones in which the ICS have been placed. The provider is obliged to retain previous versions of this file.
10.3.2. Where the provider provides electronic communications services to the public which require access to servers from external networks (such as email services), the ICS offering those services must be placed in one or more demilitarized zone (DMZ).

10.3.3. The ICS of the provider which are used by employees and associates to perform operational procedures and functions (such as management and supervision systems, logging systems, subscriber billing systems, databases retaining communications data and applications that access communications data) must be included in one or more internal trusted zones depending on the security requirements and their criticality.
10.3.4. The ICS of the provider, especially those not placed in DMZ or trusted zones (such as access/transmission networks, devices and nodes that interface with third party / external networks), depending on the technology used, may support optional use of specific security mechanisms. In this case, the provider is obliged to select, activate and configure all suitable security mechanisms, utilising the functionality and security methods they support (such as encryption), the international and widely accepted practices and standards, and the results of the risk assessment, in accordance with the principles set out in article 3.3 of this Regulation. The provider is obliged to retain a file with a complete analysis of the protection and security measures activated and configured at these ICS, for the purposes of communications confidentiality protection.

Article 11

Audit Policy for the Implementation of the Security Policy for the Assurance of Communications Confidentiality

11.1. Purpose - Scope of Policy

The Audit Policy for the implementation of the Security Policy for the Assurance of Communications Confidentiality lays down the requirements and framework for audits carried out by the provider to ensure proper compliance with the individual policies and procedures, to ascertain the adequacy and effectiveness of the security mechanisms and to check the ICS' technical vulnerabilities.

11.2. General Requirements

11.2.1. The provider should schedule the audits for the implementation of the Security Policy for the Assurance of Communications Confidentiality. The above schedule is documented and covers the entire implementation of the policy. This audit must be carried out at least every 2 years.
11.2.2. The audit should include use and examination of the log files for each ICS, and where appropriate correlation of those files with other files specified in this Regulation.
11.2.3. Audits may be carried out by an external body or by employees of the provider who have been especially authorised for this purpose.
11.2.3.1. Where an audit of the implementation of the Security Policy for the Assurance of Communications Confidentiality is carried out by an external body, care must be taken by the provider in relation to compliance with the duty of confidentiality and the non-disclosure of information and data by concluding a contract to that effect. During the entire audit by the external body, employees of the provider who have been specially authorised for that purpose must be present.
11.2.3.2. Where an audit of the implementation of the Security Policy for the Assurance of Communications Confidentiality is carried out by employees of the provider who have been

specially authorised for that purpose, they must be suitably trained and objectivity and impartiality factors must be taken into account. In particular, these inspectors must not come from the department or division whose systems are being inspected or must not have been involved in developing the code and in installing or operating the system being audited.
11.2.4. The competences of the provider's staff carrying out audits must be specified in advance and described in detail in a relevant file which is kept by the provider.

11.3. Preparation for Audit

The preparatory stages for each audit must include the following as a minimum:

i. identification of the system and communications confidentiality procedures / mechanisms which will be inspected and the audits which will be carried on to identify technical vulnerabilities;
ii. the timeframe for the audit;
iii. the data and information that needs to be collected; and
iv. the appointment of members of the audit team. The data referred to in this paragraph shall be recorded in a file which will be kept by the provider.

11.4. Audit Process

11.4.1. The stages in each audit, the relevant findings and the improvements / modifications proposed must be recorded in a special file which will be kept by the provider, even in the case where there are no findings during the audit.
11.4.2. The granting to one or more members of the audit team of access rights to software tools, systems (such as the intrusion detection systems) or to locations within the facilities must only be permitted for the duration of the audit and must be done in accordance with the provider's corresponding security policies.

11.5. Audit Findings

In case there are findings, the provider shall specify the necessary corrective actions (such as revision of procedures/instructions, updating of software, modification of technical configuration parameters, partial or total replacement of a system or application), the timeframe for achieving this, the responsibilities of employees and associates to carry out the corrective actions and the persons who are especially authorised to inspect proper implementation of the steps cited in this paragraph. Depending on how critical the findings are, the provider will activate the Security Incident Management Policy in accordance with article 9 of this Regulation.

11.6. Audit Policy for the Implementation of the Security Policy for the Assurance of Communications Confidentiality Procedure.

11.6.1. The provider must have and implement a procedure where all stages are included - preparatory, implementation; findings and corrective actions, as set out in this article and keep copies of the relevant files for all audits carried out.

Article 12

Anti-Malware Policy

12.1. Purpose - Scope of Policy

The Anti-Malware Policy must define the requirements and specify the technical and organisational measures required in order to protect the provider's ICS against malware threats and attacks.

12.2. Requirements & Obligations

12.2.1. The provider is obliged to take all necessary organisational and technical measures that seek to prevent, identify and deal with malware threats and attacks.
12.2.2. The provider is obliged to inform employees about the malware vulnerabilities and threats and their obligations in relation to security measures against malware threats and attacks.
12.2.3. The provider is obliged, in accordance with the principles of the Implementation Audit Policy of the Security Policy for the Assurance of Communications Confidentiality referred to in article 11 of this Regulation, to carry out ICS software integrity audit. That audit must seek to ascertain that there is no ICS software installed other than the software officially provided by the provider.
12.2.4. The provider is obliged to put in place suitable mechanisms to reduce the spread of malware in cases where it is identified. In that case, an immediate evaluation of the incident must be made and depending on how critical it is, the provider shall activate the Security Incident Management Policy in accordance with article 9 of this Regulation.
12.2.5. The provider is obliged to maintain a file that records the details of how the requirements of paragraph 12.2 hereof are implemented.

Article 13

Encryption Policy

13.1. Purpose - Scope of Policy

The Encryption Policy must lay down the obligation of the provider to use suitable algorithms and encryption systems to adequately protect communication data or other information which could lead to the disclosure of the communication data of subscribers or users of the networks or services provided (such as passwords and ICS structural data) during the storing and transmission of these data on/to ICS, as well as the minimum security characteristics of encryption systems. The Encryption Policy shall apply to all the provider's ICS.

13.2. General Requirements

13.2.1. The provider must implement encryption systems for ensuring the sufficient protection of communications data during their storage/transmission via networks.

13.2.2. Encryption must be applied to ICS based on the results of the risk assessment prepared in accordance with the principles set out in article 3.3 of this Regulation.
13.2.3. Where algorithms and encryption systems are used, including digital signature algorithms, international, widely accepted standards must be taken into account.
13.2.4. The length of the key used must take into account international, widely accepted standards depending on the encryption algorithm used, and the results of the risk assessment prepared in accordance with the principles set out in article 3.3 of this Regulation.
13.2.5. The provider is obliged to prevent unauthorised access to keys being used for encryption, authentication or digital signature purposes.
13.2.6. Where asymmetric encryption algorithms are used for (a) logical access to the ICS, (b) for encryption or (c) for digital signatures purposes, each public/private key pair must correspond to a unique user and the corresponding private key must be known only to the specific user to whom it corresponds.
13.2.7. Where the provider uses digital public key certificates generated by certification service providers, he is obliged to ensure that the certification service provider complies with the relevant legislation.
13.2.8. Where the provider generates and manages encryption keys used on ICS, he must prepare and comply with appropriate procedures able to create, certify, distribute and withdraw the encrypted keys.
13.2.9. The provider is obliged to keep a file that records the details of how the requirements of paragraph 13.2 hereof are implemented.

Article 14

ADAE Audit Procedure

14.1. Regular Audit

14.1.1. At regular intervals ADAE shall perform an audit to the providers falling within the scope of the provisions of this Regulation as stated in article 1 hereof. The frequency of the audits is determined by decision of ADAE.
14.1.2. The audit shall be performed by the authorised staff of ADAE in the presence of the Communications Confidentiality Assurance Officer or other authorised employee of the operator in accordance with the provisions set out below:
14.1.2.1. ADAE shall issue a decision appointing an audit team comprised of at least 3 individuals to perform an audit to the specific provider. The same decision shall also specify the members of the audit team.
14.1.2.2. At a time determined by the audit team, the Communications Confidentiality Assurance Officer will be notified in accordance with the provisions of article 3.2.6 of this Regulation about the date on which the on-site audit will be performed, and he will be expected to provide full copies of the existing procedures implementing the Security Policy for the Assurance of Communications Confidentiality approved by ADAE, which clearly indicate the date on which they were issued. Following reception of the written notice referred to in the previous indent by the Communications Confidentiality Assurance Officer about the performance of a regular audit by ADAE, and until a written notice by the Authority is received about the termination of the audit, the provider may not proceed to any revision of the texts of

the approved Security Policy for the Assurance of Communications Confidentiality or its accompanying files (procedures, technical instructions, etc.).
14.1.2.3. The audit team shall perform the on-site audit at the provider's premises in order to ascertain whether the latter is complying with the Security Policy approved by ADAE through implementing the relevant procedures. During the on-site audit the presence of the Communications Confidentiality Assurance Officer is compulsory and the audit team may request at its discretion any additional information it deems necessary. During the on-site audit the audit team cooperates with the provider's staff. The audit team shall carry out a detailed examination of the files relating to the Security Policy for the Assurance of Communications Confidentiality and implementation thereof, in order to identify any shortcomings or mismatches with the provisions of the Security Policy for the Assurance of Communications Confidentiality approved by ADAE.
14.1.2.4. A special document entitled the "Record of the Provider's Premises On-Site Audit" shall be drafted for each on-site audit and shall be signed by the Communications Confidentiality Assurance Officer.
14.1.3. After completion of the on-site audits, the audit team shall examine in detail the data collected and shall draft a special document entitled the "Provider's Regular Audit Report", which shall contain at least the following information:

a) particulars of the ADAE decision by which the regular audit was decided;
b) the name, surname and position of the members of the audit team and the date on which that team was set up;
c) the company name of the provider under audit and the name of its Communications Confidentiality Assurance Officer;
d) the "Records of the Provider's Premises On-Site Audit", and all relevant correspondence exchanged between ADAE and the provider within the framework of the regular audit;
e) a detailed description of the findings of the audit and the detection of any shortcomings or mismatches with the Security Policy for the Assurance of Communications Confidentiality approved by ADAE;
f) the date of the commencement and the termination of the audit;
g) the audit's final conclusion.

14.1.4. The Provider to which the audit was performed shall be invited to ADAE'S premises in order to receive the decision of the Plenary Session of ADAE relating to approval of the "Provider's Regular Audit Report", together with the report attached thereto.

14.2. Extraordinary Audit

14.2.1. ADAE shall perform extraordinary audits acting *ex officio* or following a complaint.
14.2.2. Extraordinary audits shall be performed without any prior warning to the provider concerned following a decision by ADAE which appoints the members of ADAE's staff which comprise the audit team. From the commencement of the extraordinary audit by ADAE and until reception of a written notice about the termination of the audit, the provider may not proceed to any revision of the texts of the approved Security Policy for the Assurance of Communications Confidentiality or its accompanying files (procedures, technical instructions, etc.).

14.2.3. While implementing the decision of ADAE referred to in paragraph 14.2.2. hereabove, the audit team may perform on-site audits at the provider's premises.
14.2.4. A special document entitled the "Record of the Provider's Premises On-Site Audit" shall be prepared for each on-site audit. The document shall be signed by the authorised provider's employees who participated in the audit.
14.2.5. After completion of any eventual on-site audits, the audit team shall examine in detail the data collected and shall draft a special document entitled the "Provider's Extraordinary Audit Report", which shall contain at least the following information:

a) particulars of the ADAE decision by which the extraordinary audit was decided;
b) the name, surname and position of the members of the audit team and the date on which that team was set up;
c) the company name of the provider under audit and the name of its Communications Confidentiality Assurance Officer;
d) the Records of the Provider's Premises On-Site Audit, and all relevant correspondence exchanged between ADAE and the provider within the framework of the extraordinary audit;
e) a detailed description of the findings of the audit and the detection of any shortcomings or mismatches with the Security Policy for the Assurance of Communications Confidentiality approved by ADAE;
f) the on-site audit date;
g) the audit's final conclusion.

14.2.6. The Provider to which the audit was performed shall be invited to ADAE'S premises in order to receive the decision of the Plenary Session of ADAE relating to approval of the "Provider's Extraordinary Audit Report", together with the report attached thereto.

Article 15

Obligation to Notify ADAE

15.1. The providers referred to in article 1(2) of this Regulation are obliged within a deadline of 2 months from the publication hereof in the Government Gazette to submit a solemn statement from their legal representative informing ADAE about:

a. the activities for which a Registration Declaration has been submitted to the Hellenic Telecommunications and Post Commission (EETT) to operate under the general authorisation regime;
b. whether they in fact carry on the activities for which the Registration Declaration was submitted to the Hellenic Communications and Post Commission (EETT), describing in detail the activities carried on and the type of ICS used to carry on those activities;
c. whether they do not in fact carry on the activities for which the Registration Declaration was submitted to the EETT, stating whether those activities were carried on in the past and for how long.

15.2. The providers referred to in article 1(2) of this Regulation are required to promptly inform ADAE in case there is any change to the network and/or service electronic communications

activities provided which they actually provide, irrespective of whether the corresponding Registration Declaration has been submitted to EETT, as well as in cases where there are changes to their corporate form, corporate name and registered head offices.

15.3. The providers shall promptly inform ADAE where there is a security incident in accordance with article 9 of this Regulation and in all cases where the relevant legislation in force requires that the authority be informed.

Article 16

Submission and Implementation of Security Policy

16.1. The providers referred to in article 1(2) of this Regulation who in fact carry on the activities for which a Registration Declaration was submitted to the EETT shall be obliged to provide ADAE the Security Policy of Confidentiality to be approved within 6 months from the date of publication hereof in the Government Gazette.

16.2. The providers referred to in article 1(2) of this Regulation who commence or change the activity or activities for which the Registration Declaration was submitted to EETT after the entry into effect of this Regulation, are required to submit the Security Policy of Communications Confidentiality to ADAE for approval, for the corresponding activities within a period of 6 months from the start of those activities.

16.3. The providers referred to in this article are obliged within 6 months from notification of the ADAE decision approving the Security Policy of Communications Confidentiality to implement that policy. Where a revised Security Policy of Communications Confidentiality is submitted, the implementation time shall be set by ADAE per case and shall be notified to the provider by means of the decision approving the Security Policy.

16.4. The providers referred to in this article shall not submit the security procedures specified in the context of this Regulation to ADAE for approval.

Article 17

Transitional Provisions

17.1. ADAE Decisions Nos. 629a/2004 of ADAE "Regulation for the assurance of confidentiality in mobile telecommunications services" (GG B'87/2005), 630a/2004 of ADAE "Regulation for the assurance of confidentiality in fixed telecommunications services."(GG B' 87/2005), 631a/2005 of ADAE "Regulation for the assurance of confidentiality in telecommunications services via wireless networks" (GG B' 87/2005), 632a/2005 of ADAE "Regulation for the assurance of confidentiality in internet communications and related services and applications" (GG B' 88/2005), 633a/2005 of ADAE "Regulation for the assurance of confidentiality in internet infrastructures" (GG B'88/2005) and 634a/2005 of

ADAE "Regulation for the assurance of applications and internet user confidentiality" (GG B' 88/2005) shall remain in effect until this Regulation enter into force.

17.2. The providers who have submitted a Security Policy to ADAE in compliance with their obligation to do so under the ADAE Regulations which are hereby repealed are required, without further notice, to submit a Security Policy of Communications Confidentiality to ADAE for approval in accordance with the requirements of this Regulation.

17.3. The providers referred to in this article shall implement the Security Policy they have submitted to ADAE in discharge of the relevant obligation under the ADAE Regulations repealed hereby until the Security Policy of Communications Confidentiality approved by ADAE in line with this Regulation is implemented, and in any event no later than the end of the deadline specified in article 16.3 of this Regulation for the implementation of the Security Policy of Communications Confidentiality.

Article 18

Entry Into Force

This Regulation shall enter into force 6 months after it is published in the Government Gazette without prejudice to the provisions of article 15(1) and 16(1) hereof. This Regulation shall be published in the Government Gazette.

Maroussi, November 10, 2011

The President

ANDREAS LAMBRINOPOULOS