PERMANENT MISSION OF GREECE
GENEVA

Ref. No. 6171.1/7/234

NOTE VERBALE

The Permanent Mission of Greece to the United Nations Office at Geneva and other International Organizations in Switzerland presents its compliments to the Office of the High Commissioner for Human Rights and with reference to the latter's Note Verbale, dated 16 January 2015 with regard to the letter of the Special Rapporteur on the right to freedom of opinion and expression, has the honour to attach herewith the contribution of the Ministry of Justice, Transparency and Human Rights.

The Permanent Mission of Greece to the United Nations Office at Geneva and other International Organizations in Switzerland avails itself of this opportunity to renew to the Office of the High Commissioner for Human Rights the assurances of its highest consideration.

Geneva, 19 February 2015

To: **The Office of the High Commissioner for Human Rights**
freedex@ohchr.org

Att.: 2 pages

1. The Hellenic Authority for Communication Security and Privacy (ADAE) was established in 2003 as prescribed by article 19 par.2 of the Hellenic Constitution, which calls for the establishment of an independent authority with the mission to ensure the confidentiality of mail and all other forms of free correspondence or communication. ADAE monitors the implementation of afl legislation relevant to the lawful interception of communications and, for this purpose, it is authorized to receive all lawful interception mandates issued by the judicial authorities.
Moreover, Law 3115/2003 attributes ADAE, inter alia, the power a) to issue regulations regarding the assurance of the confidentiality of communications, b) to perform audits on communications network/service providers, public entities as well the Hellenic National Intelligence Service, c) to hold hearings of the aforementioned entities, d) to investigate relevant complaints from the public and e) to collect relevant information using special investigative powers.

Having regard to these provisions, ADAE has issued Regulation 165/2011 "for the Assurance of confidentiality in Electronic Communications" (GG B' 2715). The provisions of this Regulation concern all persons involved in providing electronic communications networks and/or services, These entities are obliged to have and to implement a Security Policy for the Assurance of Communications Confidentiality, with a content which must be in accordance with the provisions of this Regulation. Article 13 of the Regulation, under the title 'Encryption Policy', prescribes the following:

"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 Information and Communication Systems -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 in order to ensure 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 unauthorized 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 sen/ice 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 for the creation, certification, distribution and withdrawal of 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."

2 The use of encryption tools in order to secure transactions and communications online is considered as an important security measure applied by the data controller, pursuant to article 10 on "Confidentiality and security of processing" of the Hellenic Data Protection Law 2472/1997. which obliges the data controller to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Concerning anonymity, as the processing of personal data must be necessary and performed according to the proportionality principle (article 4 of law2472/1997). the ability of individuals and organizations to employ tools to transact and communicate anonymously is encouraged from a personal data protection point of view. Prior effective anonymisation is necessary in order to further process communications data.