

Σε ανταπόκριση σχετικού αιτήματος, υποβάλλω παρατηρήσεις σχετικές με το site www.eu2003.gr που αφορά στην Ελληνική Προεδρία της Ευρωπαϊκής Ένωσης το πρώτο εξάμηνο του 2003.

Στη διάθεσή σας για περαιτέρω σχολιασμό και διευκρινίσεις.

The following recommendations focus on the data protection and privacy policy of the site of the 2003 Greek Presidency in the EU. Hereinafter the site (www.eu2003.gr) is referred to as **eu03gr**.

From a data protection perspective three major questions may be asked and the **eu03gr** must provide answers—clear and specific statements—on them:

1. What information on the Internet user's activities is generated during websurfing through **eu03gr**?
2. Where is this information stored?
3. What information is requested for services delivered by **eu03gr**?

Common data gathering:

Once a connection with the site of the Greek EU Presidency is established, the **eu03gr** collects information on the visiting Internet user. All requests to the **eu03gr** are accompanied by the destination IP-address. The **eu03gr** also knows from which page the Internet user has been transferred to it or to a page within it. The information on **eu03gr** visits is stored in the "Common Log File." This information can be analyzed to shed light upon issues such as traffic patterns to and from the **eu03gr** and the activities of its visitors.

Chattering Data:

Moreover, additional information is collected by **eu03gr** through the use of browsing software such as MS Internet Explorer; known as "Chattering Data" this information includes the operating system's identity, type and version of the user's browser, protocols used for websurfing, referring webpage, language preferences, and cookies.

Cookies:

The **eu03gr** data gathering power is enhanced through the use of cookies. These are pieces of data that can be stored in text files and put on the Internet user's hard disk, while a copy may be kept by the **eu03gr**. A cookie can contain a unique number known as "Global Unique Identifier--GUI" which allows for better personalization than dynamic IP-addresses. Cookies with GUI extend the capabilities of **eu03gr** for personalized services to its users.

Portal data gathering techniques:

The **eu03gr** operates as a portal site by containing links to other sites. Portal sites may collect information as websites in general, but they may also store information on visits to all the sites behind the portal. Provided that the **eu03gr** portal operation includes enhanced data gathering techniques, then the **eu03gr** can more easily create a complete profile of its user's online behavior.

E.T. software:

A clear and specific statement regarding the use of E.T. software¹ tools by the **eu03gr** is deemed appropriate because of the special nature of the site. E.T. software tools are monitoring applications that process personal data of users without their knowledge (invisible processing). The **eu03gr** should confirm clearly and specifically whether it does or does not deploy E.T. software tools such as Narus, Alexa, zBubbles etc to monitor its visitors' online behavior.

¹ These monitoring software applications are known as E.T. software because once they are lodged in the user's computer and learn what they want to know, they do what Steven Spielberg's extra terrestrial did: phone home.

The legal framework of EU Directives:

Directive 95/46/EC and Directive 97/66/EC apply to the lawful operation of the **eu03gr**. The **eu03gr** should be very explicit in its operation within the legal framework and the principles of the EU Directives. More specifically, **eu03gr** should explicitly honor:

- **The Finality Principle:**

Information to be provided to the data subject should in all cases contain ample and clear facts regarding the finality of the processing. Article 6 of Directive 95/46/EC prohibits the **eu03gr** from further processing of its users' data for non-compatible uses. Navigation data on its users should be collected by the **eu03gr** insofar as the data are needed to provide a service to its users, which is compatible to the purpose of its existence.

- **The Fair Processing Principle:**

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of which the data are collected. Articles 6 & 7 of Directive 95/46/EC allow the **eu03gr** to use data for other purposes than the ones for which data were collected only if data are anonymised so that it is no longer possible to link the data to the data subject. In addition and in accordance to the same principle, if data are not anonymised, data on searching and surfing the **eu03gr** should not be kept once the user's online activity has finished. This, also, means that the use of meta-tags in the components of the **eu03gr** which aim at gauging online demand for its content is not prohibited provided that the use of meta-tags does not allow for linking between query logs and the identity of the users of the **eu03gr**. In addition and in accordance to the same principle, article 6 of Directive 97/66/EC obliges the **eu03gr** to process header information—information that is 'wrapped' in several protocol headers such as TCP-header, IP-header, Ethernet-header, as traffic data in the sense of article 6 of Directive 95/46/EC.

- **The Proportional and Adequate Security Principle:**

The **eu03gr** as a provider of electronic communications services should offer adequate security measures which take into account the state of the art in the electronic communications services. These services should be proportional to the risks involved in the specific situations. Article 4 of Directive 97/66/EC describes this principle. The principle has application in the **eu03gr** and its routers and connecting lines that carry massive amounts of data.

- **The Principle of Confidentiality:**

Any kind of interception or surveillance of communications through the **eu03gr** by parties other than its users and without the previous consent of the users is prohibited. Article 5 of Directive 97/66/EC describes this principle. According to the Data Protection Working Party² surfing through different sites—thus surfing through the **eu03gr** and all its hyperlinked content (navigation data)—constitutes communication that is protected by article 5 of the aforementioned Directive.

The Safe Harbor Privacy Principles:

The **eu03gr** is designed to communication that exceeds the EU borderline. Therefore, the **eu03gr** should state respect for the Safe Harbor Privacy Principles and related FAQs issued by the US Department of Commerce in OJ 215 of August 28, 2000, regarding communication between the **eu03gr** and citizens of the US. The Data Protection Working Party has found it necessary to start considering the state of implementation of the Safe Harbor agreement³.

² Data Protection Working Party recommendation adopted 3 May 1999, 5005/99/final, WP 18.

³ Commission decision 520/2000/EC of July 26, 2000 pursuant to Directive 95/46/EC and Article 29 Data Protection Working Party, 11194/02/EN, WP62.

Technical measures for data protection:

- **Define cookies' functionality and allowance of control:**

Personal data retrieval methods are based on the use of cookies. The **eu03gr** should define cookies' functionality clearly. The visitor of the **eu03gr** should be informed on the possibility or impossibility of browsing and using the **eu03gr** with or without enabling cookies in his/her browser. The statement on cookies should be explicit regarding users' allowance to control cookies of first-party and third-party⁴.

- **Define proxy server's functionality regarding hide of IP-number:**

It is possible for the **eu03gr** to make use of a proxy server in order to hide the IP-number of its visitors by referring to it through the proxy server. In that case, only the masqueraded IP-number of the proxy server is transmitted, while the address of the visitor is kept with the **eu03gr**. It should be clearly stated, if this option for enhancing privacy and data protection is available.

- **Define "trusted party" portal operation:**

It is possible for the **eu03gr** to undertake the role of a "trusted party" portal regarding the contained hyperlinks to other sites, especially those of the public sector. In that case, the **eu03gr** operates as a guard regarding its visitors' personal data when they visit hyperlinked sites through it. It should be clearly stated, if this option for enhancing privacy and data protection is available.

- **Define anonymisation software functionality:**

It is possible for the **eu03gr** to deploy the use of anonymisation software tools to hide its visitors' IP-address. The **eu03gr** may redirect communication to it across dedicated servers that substitute its visitors' IP-addresses with another. The notion of "pseudo-identity" could offer an alternative solution for balance between legitimate use of the **eu03gr** and protection of personal data. Such an identity could be attributed to a visitor through the **eu03gr**. It should be clearly stated, if this option for enhancing privacy and data protection is available.

- **Define the processing protocol for newsgroups or chat:**

The usual processing protocol for newsgroups is the NNTP (News Network Transfer Protocol); some newsgroups also use the HTTP protocol. The NNTP processes permanent connections between newsgroup servers and updates messages automatically. The **eu03gr** should define which protocol is used for its newsgroup utility because data mining breach of data privacy can happen in the Internet through software that can search the Internet and collect all available data about a person who may participate in a newsgroup⁵. The Council of Europe Recommendation # R (99) 5 for the Protection of Privacy on the Internet⁶ requests that newsgroup service providers should inform their users of the privacy risks associated to newsgroup communication services. In addition, all the provisions of Directives 95/46/EC and 97/66/EC apply to newsgroup communication.

- **Define the use of Robot exclusion protocol or Robot Meta-tags:**

Robot exclusion protocol may be used to prevent all or some of the pages of the **eu03gr** from being automatically indexed by a search engine. Robot Meta-tags may be used by creators of hyperlinked to the **eu03gr** sites if they wish to prevent their sites from being indexed automatically by a search engine. It should be clearly stated, if this option for enhancing privacy and data protection is available.

⁴ Persistent third-party cookies are heavily used by Internet advertisers to track computer users' activities online behavior.

⁵ According to the recommendation adopted by the Data Protection Working Party on December 3, 1997, identifiable ... data by its very existence creates a means through which individual behavior can be surveyed and monitored to a degree that has never been possible before.

⁶ Recommendation of the Committee of Ministers to Member States adopted on February 23, 1999.