



---

"This project has been funded with support from the European Union. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

## **Resolution:**

### **Data Protection and Internet Security**

*Adopted at the YEPP Council in Marseille on 10<sup>th</sup> December 2011.*

Data protection and fundamental safeguarding of privacy rights of EU citizens is of great importance to the European Commission, and, subsequently to the Youth of the European People's Party. The advent of new technologies, the tightly interlinked cyber society and the heterogeneous law enforcement strategies in EU member states allows for increased concerns of EU citizens over their fundamental right of privacy and data protection. The European Commission has drafted and issued the Directive 95/46/EC, in 1995 which aimed at protecting citizens from becoming victims of data theft and opaque misappropriation of personal, privileged information. The aforementioned directive, even though outdated, has shed much needed light on the issue, with regards to actions relating to buffering and preventive schemes which, if accurately implemented can result to a more secure data protection framework. EC's Directorate General for Justice organized a public consultation about the future legal framework for protecting personal data and procured a report in November 2010. Citizens, as well as formal private and public organizations participated in the consultation in an effort to update the existing framework in matters of technologies and previous definitions.

In order to portray the significance of the issue, one would need to refer to public opinion. According to the 2008 Euro-barometer analytical report on "Citizens' Perceptions; Data Protection in the European Union", the EU27 average frequent computer usage nears 85%. Countries like Denmark and the UK respective percentage reaches up to 97%. On the matter of transmission of data through the internet, the responses were quite different. Nearly 85% of respondents admitted that they do not feel confident with the current level of security with regards to data processing and internet privacy. Greek, Italian, Spanish, German and Slovenian respondents, approximately 90% of them, do not feel that the current internet privacy and security framework is sufficient. Moreover, awareness levels of technologies and tools that computer or internet users can employ so as to safeguard their personal information is quite low. Approximately 56% of EU-wide respondents admitted that they don't know how to use internet firewall, cookies and filtering tools. The awareness deficit, as well as the existing legal framework can foster illegal data acquisition from third parties therefore rendering EU citizens incapable of protecting their personal information.

Considering the current need for further elaboration, YEPP presents its resolution on data protection and internet privacy by **acknowledging**:

1. the right of computer/internet users to anonymity while at the same time their fundamental right to privacy of personal information and related data security,
2. the progressive rhythm of technological development which has allowed for applications and tools to be able to retrieve third party data and information,
3. the inadequacy of the existing security framework to battle innovative techniques of target advertising and profiling, which is a product of data warehouse processing, therefore limiting the security of IP addresses,
4. the diverse data protection legislation among EU Member States which does not allow for centrally coordinated and consolidated legal prosecution of security breach strikes,
5. the need to update definitions of the Directive 95/46/EC with regards to protection of individual information and the fundamental right of privacy, due to the advent of new technological tools and applications,
6. the faster, cross-border, transmission of data (EU and non EU countries) which poses as a heavy administrative burden for organizations wishing to align to EU data protection directives and certifications,
7. the narrow scope of the aforementioned EC Directive which does not include information made available on the internet to an imprecise number of people,
8. that upholding the fundamental right of privacy should coincide and be balanced against other fundamental rights of individuals such as that of property and freedom of economic activity whilst safeguarding security of data processing,

**The Youth of the European People's Party Calls on:**

1. EU Member States to implement awareness campaigns with regards to:
  - i. Internet security and possible data manipulation,
  - ii. Existing tools and applications, and how individuals can use such means to protect themselves from potential hazards;
2. the European Commission, in collaboration with experts, to modernize the provisions of the Directive 95/46/EC pertaining to data protection and security so as to be applicable to new technologies and applications (e.g cloud computing);
3. EU relevant institutions to monitor the cross-border and cross-sector transmission of data and information so as for the allocation of accountability, responsibility and liability to be effective and just in cases of privacy breaches;
4. Member States to steadfastly move towards further cohesion of national data processing legislation in order to:
  - i. stabilize internal market data exchanges, and,

- ii. refrain from imposing further administrative burdens on companies that wish to align their practices to the different regulations wherever the location of their operations;
- 5. The composition of a Data Protection Agency which will be comprised of independent experts and representatives of the fields of information technology and legislature, aiming at legitimizing the safeguarding of citizens' and organizations' data;
- 6. the EC to enforce a certification strategy which will provide formal credentials to organizations that take on the challenge to align their data processing with the aforementioned directive;
- 7. EU institutions to collaborate with organizations of the private sector in law enforcement practices towards realizing the efforts of safeguarding citizens' privacy as proposed by the Directive itself;
- 8. the EC to require from organizations , whether private, public or individual entities, to clearly define an internal accountability chain in cases of data processing and transferring in order to encourage self-regulation with regards to potential privacy and security breaches.