Unit C3 – Data protection
Directorate-General Justice
European Commission
B-1049 Brussels, Belgium

Email: JUST-PRIVACY-CONSULTATIONS@ec.europa.eu

Vienna, January 12, 2011

ISPA CONTRIBUTION REGARDING PUBLIC CONSULTATION ON THE COMMISSION'S COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

ISPA (Internet Service Providers Austria; Identification Number: 56028372438-43) is pleased that the Commission has initiated this consultation process on the Commission's comprehensive approach on personal data protection in the European Union.

We are convinced of the need to preserve the principles-based approach of the Directive as it provides the flexibility required to face future technological developments as long as a coordinated approach is adopted on an EU level.

Furthermore we acknowledge that it is important to address the impact of future innovations on privacy through non-legislative measures, such as the use of privacy-enhancing technologies (PET), privacy by design and industry self-regulation. We are convinced that such measures are the most effective approaches to deal with fast moving-technology markets. Legislative measures on the contrary which are not technology-neutral could instead act as a barrier to innovation and competition, depriving consumers of valuable products and services.

ISPA would like to stress that data protection rules should however be applied horizontally to all economic sectors and actors processing personal data which have an impact on the privacy of individuals. A level playing field is crucial to build uniform expectations and experiences online while increasing the confidence on using online services. We explicitly welcome the reference in the Commission's Communication to sensitive data, privacy information notices and the extension of data protection rules also onto the area of police and judicial cooperation on criminal matters.

1. Privacy rules in Europe suffer from a lack of harmonisation

The Directive has - as also acknowledged by the Commission in its Communication - failed to create a harmonised framework across the EU. Member States have implemented the provisions of the Directive in divergent ways with the consequence of thus creating obstacles to the establishment of the Single Market.

The efforts of the Article 29 WP in the achievement of a consistent interpretation of the provisions of the Directive are highly welcomed but have not succeeded in preventing a fragmented application of the Directive. For example § 4 Z 3 of Austria's Data Protection Act, other than the corresponding German Act, covers not only the personal information of natural

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

persons (‘*natürliche Personen*’), but also explicitly mentions the personal information of legal entities (‘*juristische Personen*’).

Bureaucratic obstacles, arising out of diverging national laws, pose an obstacle to the free movement of data and inhibiting the development of cross-Member State services such as e.g. cloud computing. ISPA believes that in a fully harmonized privacy framework data controllers would not be prevented from moving data freely within the EU. Any such restrictions are contrary to the obligations imposed onto the Member States by Article 1 (2) of the Directive 95/46/EC.

2. An increasing degree of harmonization reduces the importance of the question of the applicable law

The definition of the applicable law is a key question in a globalised online environment, where a fairly common scenario is the collection and processing of data belonging to European citizens by entities outside of the EU. Article 4 of the Directive 95/46/EC already addressed this issue stating that the Directive is applicable to data processing anywhere and, therefore, also outside the EU if (a) the controller is established in the EU, or if (b) the controller is established outside the EU but uses equipment in the EU. This might lead to problems where a data processor is not using equipment in the EU or is not established in the EU (e.g. Facebook).

3. Transparency is the key for raising user awareness

ISPA agrees that transparency is a fundamental prerequisite for enabling individuals to exercise control over their own data and to secure the effective protection of personal data. We agree therefore that it is essential for individuals to be well and clearly informed by the data controllers. Such information must be easily accessible and easy to understand. ISPA is of the opinion that any new or amended legal framework covering this issue must address the responsibilities of all actors across the global information ecosystem and also has to take into account the international dimension of products, services and information flows.

4. Increasing education efforts for minors are essential

ISPA stresses the importance of informing data subjects about the privacy impact of their behaviours in the online environment (e.g. behavioural advertising). In order to make data protection rules fully effective, education and awareness-raising initiatives should be promoted by both public and private sectors. Member States are already obliged by Article 14 of the Directive 95/46/CE to ensure data subjects are aware of their rights. ISPA is of the opinion that national Data Protection Authorities (DPAs) via the Article 29 Working Party should extend their positive working relations with key stakeholders to understand the degree to which further awareness raising is needed and how it may be improved.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Young people in the online world are becoming increasingly aware of the privacy implications and consequences of engagement, and are actively managing their privacy. ISPA is therefore of the opinion that emphasis should be put on awareness and education efforts i.e., the EU-wide Safer Internet campaign and self-regulatory approaches to specific services or contexts that may impact on the privacy of minors, combined with co-regulatory guidance that promotes a harmonised approach.

5. Equal and effective data breach notification for all industry sectors

The revision of the Directive should be welcomed as an opportunity to amend and simplify the data breaches notification process and extend security breach notification requirements equally to all sectors, including for example, law enforcement agencies, online banking, schools, and health services.

ISPA is of the opinion that security breach notification requirements should be further harmonised and applied irrespective of the jurisdiction of the responsible person. It is important that a detailed engagement begins with consultations with key stakeholders through an expert group to ensure a pragmatic, harm-based approach. The focus of such experts groups should lie on exploring the following issues:

a. What data types should the obligation for a data breach notification apply to?
b. What type of harm and thresholds of harm should be applied?
c. Should the obligations apply to data that has been encrypted or only to unencrypted data?
d. What will be the role of national data protection authorities and their jurisdiction over such matters?
e. How should the timings of notifications to DPAs and/or individuals be set?
f. Who should notify the data subjects: the data controller or the DPA?
g. Should the requirements also apply to the ‘unlawful destruction’ or ‘alteration’ of data?

6. Enhancing users’ control over their data

The right for the individual to request deletion of his/her personal data already exists under Article 12 of Directive 95/46/EC which provides individuals with a qualified right to request their personal data be rectified, blocked or erased. Some Member States have implemented the Directive in ways that obliges data controllers to meet such a request unless there is a justified reason for not doing so. This regime is supported by redress mechanisms which gives the individual the right to ask the data protection authority to assess the refusal of requests to erase data and which also gives the individual the right to pursue any such refusals via the courts.

ISPA considers this framework generally satisfactory, but is of the opinion that it should be strengthened by establishing more precisely the principle of accountability not just for data controllers, but for DPAs and the judiciary as well. E-communications services providers are already subject to strict rules under the e-Privacy Directive 2002/58/EC which requires such

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

providers to delete or anonymise communications data when those data are no longer needed for legitimate business purposes.

Furthermore ISPA supports the concepts of '*the right to be forgotten*' as well as the concept of '*data minimisation*', which is already laid down in the Directive 95/46EC.

7. No additional regulation for data portability needed

Data subjects should have the right to withdraw his/her own data from an application or service so that the withdrawn data can be transferred into another application or service, if technically feasible, without undue hindrance from the former data controller. Such a right already exists as individuals have the right of access to their personal data and to be given a copy of that data pursuant to Article 12 of Directive 95/46/EC. ISPA thus does not see any need for further regulation in this field, but acknowledges that further investigation is required to ensure such rights can be exercised irrespective of the location of the data controller and to reflect the global nature of Internet services.

8. Explicit consent should only be required when necessary and feasible

ISPA is of the opinion that effective, '*future-proof*' data protection rules should not impede, but rather foster the development of new services while at the same time supporting a uniform privacy framework for users. In our opinion over-regulation and over-protection are not the way to achieve effective data protection.

ISPA is concerned that requiring explicit consent for all processing will effectively undermine privacy. Privacy in our opinion is dynamic and contextual, not static. Rather than focusing on consent at the expense of other opportunities to enhance a user's privacy experience, we believe that a key objective for data controllers should be to develop mechanisms by which users, depending on the context of specific uses of data, can make informed choices.

For example, a person requesting a location based information service to locate the nearest subway station, is actively asking to be located, and should thus not be required to negotiate cumbersome, lengthy legalistic privacy notices by which they may indicate their 'unambiguous explicit consent'. Making users repeatedly consent to such privacy notices for each use will lead to the fact that users will effectively start to ignore them. Thus such impositions would not only impair user experience but at the same time and do little, if anything, to enhance the user privacy experience.

In case however that the location based service provider should wish to retain information about the use of the service for e.g. the purposes of targeting the user at a later stage with offers, then the service provider should be expected to provide the user with contextual notice about this measure and ensure the user is able to express his/her choice and preference.

ISPA acknowledges the need to avoid ambiguous and confusing information or even an absence of information but it however does not accept that consent in any cases has to be prior. With regard to the e-communications sector, and after long discussions during the

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

adoption process of the Directive 139/2009/EC on e-Privacy, the legislator agreed that the final text should not include the word '*prior*'.

9. Self regulation is a powerful and timely way to address privacy issues

ISPA is of the opinion that self-regulation based on a privacy-by-design approach, which includes the principle of accountability and recognises the dynamic contextual nature of privacy, can work to ensure that individuals are both aware of and able to exercise their various rights. In our view, self-regulation is in a position to respond in a more timely and effective manner to changes in technology and business models than ex-ante legislation. However, in order to develop self-regulation, further harmonisation and clarity of rules among Member States is crucial.

ISPA believes that if the Commission intends to actively promote self-regulation or EU certification schemes, this should be done in close cooperation with the industry through an expert group to ensure a pragmatic approach.

10. Addressing the need for a clear sharing of responsibility between data controllers and data processors

The distinction between data controller and data processor is changing, increasingly blurring in the online environment and is becoming outdated with the development of services such as e.g. cloud-computing, outsourcings and sub-processing. Frequently it can be noticed that several parties are defined as '*joint data controller*' as they determine '*the purposes and means of the processing*' (Article 2 of the Directive). In order to adequately address these changes, ISPA believes that the data controller's rules of liability should be made more flexible to allow contractual clauses with data processors that clearly outline where the liability lies as in many circumstances the data processor is the only party responsible for the data security and quality.

11. Clear rules on intermediary liability are a key necessity

Intermediary liability protection is fundamental to the viability of the Internet as it exists today. The Electronic Commerce Directive (ECD) determines the conditions by which intermediaries' liability of access providers or hosting providers is limited. Any platform that hosts user-generated content (including online social networks) relies on protection from intermediary liability for its survival. In many instances intermediaries are processors and, therefore, acting entirely on behalf of the data controller. In those cases, it should be clear that the ultimate responsibility to assure compliance with the data protection law relies on the data controller.

Unfortunately, the ECD does not extend to privacy and data protection aspects, nor was the concept of intermediaries considered when the Data Protection Directive was drafted. As a result, intermediary liability in the EU for cases of privacy and data protection is not subject to harmonisation which led to the risk that Member States can hold intermediaries liable for data protection violations, regardless of the circumstances of the case.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

We believe that failing to recognize the role of intermediaries could lead to a general obligation for intermediaries of monitoring the Internet. Such outcome has already clearly been ruled out in the ECD, because it would seriously hamper the viability of the Internet and because it could have implications on privacy that outweigh the aims of such monitoring. Therefore, we call on the Commission to explicitly state in the text of the revised Directive that intermediaries should not be considered data controllers for the purposes of the Directive.

12. Reducing the administrative burden regarding the notification of processing of personal data

The obligation on data controllers to notify Data Protection Authorities (DPAs) of the processing of personal data amounts to an increase in the administrative notification duties without any real advantage for data subjects. ISPA is of the opinion that in order to address this concern, possible solutions could be considered such as a mutual recognition of a notification by a DPA in a country. This would make further steps in other Member States unnecessary and thus allow a reduction in resource-consuming notification processes while at the same time assuring that this will not lead to a 'race to the bottom' within the Member States". Another way of reducing the burden of the notification obligation would be by adopting and where already existing, expanding the possibilities provided in Article 18 (2) of the Directive (Exemption from notification).

13. Including enforcement agencies into the privacy framework will increase the overall data protection benefit

ISPA would like to put emphasis on the fact that e-communications providers are currently facing high administrative burdens, associated with compliance costs due to differences between processes in each of the Member States. On the other hand, the benefit of strong data protection rules to consumers is not being maximised, because enforcement resources are not focused on the avoidance of consumer harm. We believe that if DPAs were able to adopt a more outcome-focused approach and a lighter administrative burden, consumers would be better protected by the framework.

Additionally, Internet Services Providers (ISPs) should not be put in situations of undue liability for data requested by and subsequently provided to national law enforcement authorities. The relevant authorities at the same time should be bound to take clear responsibility for the economic costs to ISPs of data retention and provision, and should also be clearly responsible for any consequences for civil liberties or Human Rights violations.

14. Strengthening the role of the Article 29 Working Party is essential

ISPA believes that this review provides an excellent opportunity to define a better interpretation of the legal framework which takes into account not only the Internal Market

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

dimension but which also puts privacy legislation into the context of other EU policy objectives and instruments.

We therefore acknowledge efforts of the Article 29 Working Party to achieve an increased harmonisation and coordination in the application of the Directive. However, we believe that, in order to achieve such a goal, the Commission needs to be given more interpretative powers, while still taking advantage of the advisory role of the Article 29. We also consider that further involvement of the private sector in the activity of the Article 29 is necessary.

The Article 29 working party should be more transparent and accountable for the decisions and opinions adopted, and should seek to ensure views of key stakeholders are considered wherever possible. The Article 29 working party should furthermore be required to assess the degree to which the data privacy Directives have been interpreted and applied in ways that achieve harmonisation across Member States and to publish the findings of such assessments to aid the Commission in its decision making.

15. Conclusions

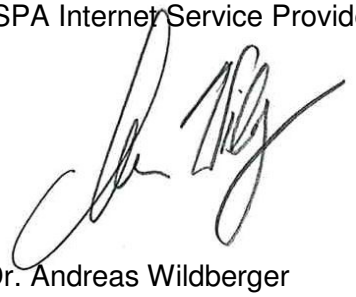
ISPA fully acknowledges that the Directive 95/46 has played a crucial role in protecting the rights of individuals and offering mechanisms for businesses to maintain consumer confidence. Nevertheless, the divergences in implementation across Member States have raised barriers for the completion of the Single Market. However, a flexible framework which allows businesses to create and offer products and services at an international level, while ensuring that data subjects maintain their right to an efficient data protection through effective enforcement and accountability mechanisms, has not yet been achieved.

It is critical that Europe avoids the temptation to address the challenges of the global Internet by walling itself off as this would constitute a grave error and would at the same time undermine the very core of the value of the Internet to foster innovation and provide the infrastructure for a truly global offering of competitive products and services to an empowered consumer.

For further information or any questions please do not hesitate to contact us.

Sincerely,

ISPA Internet Service Providers Austria



Dr. Andreas Wildberger
Secretary General

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

About ISPA: ISPA is the Austrian association of Internet Service Providers, representing approximately 200 ISPs. ISPA is a major voice of the Austrian Internet industry. Our goal is to shape the economic and legal framework supporting optimal growth of the Internet and Internet services. We regard the use of the Internet as an important cultural skill and acknowledge the resulting socio-political responsibilities.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977