RESPONSE TO EUROPEAN COMMISSION CONSULTATION ON THE LEGAL FRAMEWORK FOR THE FUNDAMENTAL RIGHT TO PROTECTION OF PERSONAL DATA

EXECUTIVE SUMMARY

The EU’s Data Protection Directive has provided a flexible legal framework. The Directive’s fundamental principles, its technology neutral character and flexibility made it a future proof and reference legal framework. It has raised the bar for data protection, and ensured a level of harmonization and awareness.

The follow up to the review should focus on better implementation, harmonization and communication of the Directive. The Directive’s principles are not broken. However, there are several issues that need to be resolved via better implementation, harmonization and communication.

DIGITALEUROPE therefore proposes the following recommendations for further improvement:

- Administrative procedures should be streamlined. Focus should be placed on data protection authorities providing guidance on how to comply with the law and conducting ex post assessments where needed. Companies incur costs on administrative procedures that could be better allocated to substantial data protection measures.

- Governments should make sufficient resources available for a robust, predictable and harmonised enforcement of data protection laws. Enforcement by public entities should be more harm-based, focusing primarily on adverse effects to the privacy or the fundamental rights of European citizens.

- Divergent implementation of EU data protection law should be avoided and cooperation on an international level is needed to create a favourable and consistent regulatory environment for the European digital technology industry.

- The international data transfer regime should be simplified. Companies should be able to certify their handling of data on a worldwide basis, as long as adequate safeguards are in place for the fair processing of the data. A privacy governance model based on accountability could help achieve this.

- Public-private co-operation should be improved. Co-operation between government agencies, industry and organizations that provide privacy and trust services is highly desirable so as to establish good practices in the areas of both privacy and security.
1- INTRODUCTION

DIGITALEUROPE welcomes the opportunity given by the European Commission to contribute to the discussion on the “The Legal Framework for the Fundamental Right to Protection of Personal Data”. The cornerstone of the EU’s protection of privacy as a fundamental right is the Data Protection Directive (hereafter “the Directive”) which has provided a fundamental framework for data protection in the European Union by ensuring that Member States provide an environment in which users and citizens would feel comfortable participating in the digital society, while their right to privacy is respected and they trust the use of technology.

Since its inception, continuous innovation in new technologies has enabled a digital revolution with the development of a critical mass of “digital citizens”. We are increasingly connected and a global data flow is essential for today’s information economy. The Directive’s fundamental principles, its technology neutral character and flexibility have provided a sufficient framework for this transformation to a “Digital Europe”. However, there is room for improvement and modernizing the data protection environment for the global world.

DIGITALEUROPE recognizes that there are a number of ways forward following review of the Directive:
   a) keep the status quo;
   b) complete overhaul or minor revision with selected amendments;
   c) additional specific Directives, and;
   d) reinforced coordination of national approaches at European level.

DIGITALEUROPE is not suggesting that the European Commission should undertake a (major or limited) recast of the Directive. We think that the focus should be on achieving more harmonization, better implementation and consistent enforcement, and on moving towards a more outcome-based system, rather than merely focusing on inputs. Ultimately, we believe this approach will achieve better levels of privacy protection for European citizens.

DIGITALEUROPE is looking forward to continuing the dialogue between government, privacy organizations and industry on how to further improve the implementation and interpretation of the data protection framework in Europe and at a global level. The ultimate goal should be the creation of an environment where users can further trust their use of technology, fostering technological innovation and enabling continued consumer benefits.

---

2- CHALLENGES ON THE ROAD TO A DIGITAL EUROPE

The emergence of a Digital Europe thanks to new technologies has created different opportunities but also the need to better understand the challenges to security and privacy. We are concerned about some of the implementation and process issues related to the Directive, especially in the areas of implementing new technologies, establishing fluid international business processes, allocating jurisdiction and responsibilities, and the challenge of conflicting legal obligations around the world. This means that current privacy and data protection rules are creating confusion amongst citizens and industry. Some of these challenges are listed below:

International data flows: At the time the Directive was adopted, most data transfers occurred in the context of Electronic Data Interchange (EDI), a point-to-point interchange of information often used for batch processing and return. Since its inception in 1995, increased mobility and modern communication and information technologies have created global data flows which have brought significant benefits to consumers around the world. At the same time a less predictable data flow environment has emerged, where global companies provide services to highly mobile and globally-based customers – services which are of increasing complexity and which incur increasing compliance costs. As services increasingly move to the cloud, data flows will become even more continuous and multi-point and regulatory models need to accommodate this change in global information flows.

Accountability: It has increasingly become a challenge to define accountability in a time where the interaction of technologies and organizations intermingle to support global and individual needs. All stakeholders should have an equal role with a need for more clarity and ownership of responsibility. Any review of the Directive should take into account the need to encourage the development of even more accountable organizations consistently upholding the protection and rights of individuals, instead of merely seeking legal compliance. Ensuring that this accountability follows the data, regardless of where it is controlled or processed, will ultimately benefit all consumers.

With the opportunities and consumer benefits that accompany this new digital life come new risks, including more sophisticated computer-related criminal exploits of which consumers are only now becoming aware. New trust and business models related to the digital economy are still emerging and consumers are still adapting to how to evaluate risk and reputation in the information society. Companies, governments and individual users all have important roles in better understanding these risks and adopting behaviours appropriate to their function so as to help address the risks.

DIGITALEUROPE members are committed to building the user’s trust in ICT, and we realise this is intrinsically connected to the growth of the ICT sector. Therefore, we have to look at the various elements associated with trust and ensure we are making progress on each of

\* A recent paper from "The Privacy Projects - TPP" on "Managing Global Data Flows: Cross border information flows in a networked environment" provides a good overview of different data flows in 6 companies. For more information: www.theprivacyprojects.org.
these. Privacy is an integral part of building user trust in technology and our main focus. Thus, we would like to share some of our initial observations on the Directive’s functioning, based on the experience of our members with the Directive’s requirements and those of other privacy frameworks.

3- THE DIRECTIVE – A COMPREHENSIVE FRAMEWORK OF PROTECTION

The Directive is based on the fundamental principles that serve as the foundation of other established approaches, and has provided a mechanism of harmonization of divergent data protection legislations. One of its most important characteristics is its technology neutral character which allows it to respond to technological developments in a flexible manner. Although there is still room for improvement, it has several strengths which make it a comprehensive framework of protection of the user’s fundamental right to privacy:

**Fundamental principles:** DIGITALEUROPE members fully support the Directive’s underlying principles, which also serve as the foundation of the Council of Europe’s Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data\(^5\) and of the OECD’s Privacy Guidelines\(^6\) which have served to improve awareness and understanding of data protection concerns. These fundamental principles are still valid and have emerged as a leading global paradigm for privacy protection.

**Harmonization:** Having realised that diverging data protection legislation in the EU Member States impedes the free flow of data within the EU, the European Commission decided to harmonize relevant laws and launched its proposal for what eventually became the Directive. One of its main achievements has been its effect on harmonization, although – as will be outlined later - we believe that still greater consistency can be achieved. Harmonized data protection laws contribute to the strength and attractiveness of the European market and create greater efficiencies for both the public and private sector.

**Technology neutral character:** The Directive’s technology-agnostic approach provides a broad framework which can be applied to different (also nascent) technologies. It enables rather than stifles innovation and does not discriminate against any one technology. Any future follow up to the review should take into account that the technology neutral character is the cornerstone of the Directive and, therefore, must be maintained in any future action from the EC.

**Direction setting:** The Directive gives people important and usable rights and has served as a reference point for good practice. It has helped protect users and ensure that privacy is viewed as an important value. The Directive’s guidelines have served as the “high bar” and reference point for organizations across the globe in terms of developing and enforcing privacy policy.

---

4- OPPORTUNITIES FOR A MORE EFFECTIVE DIRECTIVE

Although great progress has been made since its inception, the Directive still faces issues regarding its implementation, interpretation and communication. The underlying principles must be applied to new business realities and new technologies. The application of some of the requirements, such as the obligation to inform the data subject and the restrictions on data export, is unclear in light of new technologies and global information flows. This means that companies are increasingly becoming uncertain of their legal obligations.

The legal framework should strengthen and support the evolution towards even more (public and private) accountable organizations that are focused on upholding the protection and rights of individuals rather than merely seeking legal compliance. The Directive already offers a tool-box to achieve such an evolution towards a more accountable system that focuses on output rather than ex ante compliance, backed up by more efficient enforcement, increased harmonization, development of good practices and investments in a higher level of cooperation between all stakeholders.

4- 1- From ex ante to an outcome-based system

Legislation should aim at focusing industry and government resources on creating a system of trust in participation in digital life. Bureaucratic ex ante compliance procedures such as registration and notification, prior checking and data export authorizations create burden without commensurate benefit. The underlying principle should be the move towards a more accountable system.

To that end, we believe that bureaucratic ex ante compliance procedures should be phased out in favour of more flexible, risk-based processes that are more complementary to new information models and business processes. We believe that this flexible, risk-based approach would be more effective in meeting the main objectives of data protection legislation. As it may take some time to move from ex ante compliance procedures to more flexible, risk-based processes, we would suggest that actions be undertaken in the short term to harmonize these requirements to the extent possible to limit the needless duplication and complexity of filing. Opportunities for such actions are simplified notification requirements, more harmonized appointment of DPOs and realistic solutions for international data transfers.

Simplified notification: the rationale behind notification is to enable authorities to better understand the nature of data processing which is important for reasons of transparency and accountability. However, the prior checking and approval of processing of personal data has become overly bureaucratic and unsustainable given the aforementioned increase in global data flows. Companies already engage in risk analysis related to processing, which includes consideration of factors such as the nature of the data as well as the type and location of data processing. It would be better to develop systems that work in a manner complementary

---

7 Examples of new technologies relevant here include web 2.0 technologies, business process outsourcing, software as a service and cloud computing.
to systems already established by businesses. This more flexible approach would not only decrease costs and burdens, freeing greater resources for privacy protection, but would better align the interests of both companies and data protection authorities. One example of how to achieve such simplification, while at the same time safeguarding the objectives of the Directive, is the appointment of Data Protection Officers (DPOs).

**Appointment of DPOs:** The Directive codified the exemption where a company names an official who is a contact point for the regulators in one or more Member States. The DPOs have a great understanding of the different business processes and their designs and data flows and have the responsibility to ensure a robust and functional compliance program, one tailored to the size and scope of the particular company. Such DPO appointments should be more encouraged by allowing organizations that have installed such positions and provided their contact details to the Data Protection Authorities (DPAs), to be exempt from registrations and notifications. Requirements regarding the official’s qualifications should be flexible to allow companies to appoint the appropriate person for this position, meaning that there should be no restrictions on country of citizenship, language ability, or a mandatory certification system. However, voluntary certification would be welcome in the context of creating accountable organizations.

DPOs should not be personally liable or potentially criminally responsible, expect for cases of clear and intentional fraud towards the DPA.

At the same time, this would be a great opportunity for DPAs to devote and re-assign resources to working with DPOs on outreach and education and jointly work towards a more accountable system instead of focusing on mere ex-ante exercises.

The opportunity as provided for by the Directive unfortunately has not come to full fruition given that there is a great variation in the implementation of this exemption in the Member States. There should be more harmonized implementation of this provision and a drive to institutionalize DPO education, for example by way of voluntary Europe-wide data protection expert certification, thereby creating a true privacy profession, thereby creating a true privacy profession.

Companies should, however, be able to demonstrate their ability to comply with relevant data protection requirements also through other suitable alternatives instead of installing a DPO. For example, a certification approach of evaluating an organization in terms of its data privacy practices and based on mutual recognition is seen as one example alternative to mandating DPOs. Binding corporate rules (BCRs) could serve as one mechanism of such certification.

**International data transfers:** Today’s EU citizens lead a growing portion of their daily lives in a physical and virtual world that routinely crosses borders within the EU and around the world. Companies should be able to certify their handling of data on a worldwide basis, as long as the parent company agrees to ensure that adequate safeguards are in place for the fair processing of the data. Regardless of the country in which the information is processed or stored the transfer of information should not be prohibited, provided that the company complies with and remains accountable to the applicable legal requirements. Accountability

---

8 Art. 18.2 Data Protection Directive.
as a privacy governance model is preferable and more workable than an adequacy standard. Positive moves in this direction include the evaluation processes inherent in the BCR process. However, the BCR approval process should be improved by making sure it is less burdensome and there is more transparency regarding the additional DPA requirements at national level and extending the mutual recognition of a lead DPAs’ approval to all Member States.

There are still differences pertaining to the requirements and procedures of the use of Model Contracts for the transfer of personal data to third countries on a national level, for example in terms of what level of detail is required to describe the data transfer in question. To the extent the Model Contracts for the transfer of personal data to third countries remain a tool for international transfer of personal data, a more harmonized approach across Member States would benefit data controllers without detrimental effect to the data subjects.

These are some examples of opportunities for more uniform approaches complementing existing functions and processes within companies and providing more efficient avenues towards compliance. As information flows continue to expand and change in nature, *ex ante* registration requirements will demand such a level of filing that will constrain and burden not only compliance budgets of companies, but also enforcement and operating budgets of data protection authorities.

**4- 2- Enforcement and necessary oversight**

A move towards a more accountable system would allow governments to make sufficient resources available for a robust, predictable and harmonized enforcement. This enforcement should be more harms-based, focusing primarily on adverse effects to the privacy or the fundamental rights of European citizens. Supporting other private sector organizations, whether commercial or not-for-profit entities, in setting up and handling alternative dispute resolution procedures with a clearly defined scope and escalation process to regulatory authorities would enable government authorities to allocate enforcement resources to the most important and complex compliance issues.

Applying multiple and divergent national data protection laws to the same data process must be avoided. Jurisdiction and enforcement should be facilitated by mutual recognition and international cooperation.

**4- 3- Harmonization – need for increased implementation and harmonization**

As mentioned earlier, one of the Directive’s main achievements has been the start of a harmonization of Member State legislation. At the time a great step forward, additional impetus is greatly needed as differences in its implementation by the Member States are still a cause of concern. This was already acknowledged in the first review undertaken in 2003 by the Commission, which stated that “[the Commission] thinks that stakeholders are right to demand more convergence in legislation and in the way it is applied by the Member States and the national supervisory authorities in particular”. Differences between the Member States are still a cause of concern.

---

States with regard to the interpretation of the Directive and how it should be applied still exist. This means that the right balance between data protection and free flow of information has not been achieved yet, which is undermining the overall goal of ensuring compliance with the Directive’s principles.

As a consequence, the Directive’s objective to protect the fundamental right to privacy and data protection has become the subject of highly specialized legal expertise. The substantive rules of the Directive should be more self-evident so that businesses, employees, and consumers better understand their privacy rights and obligations, and unnecessary compliance costs are avoided.

The relationship between this Directive and other privacy frameworks outside the EU also needs to be reviewed, to ensure the free flow of information at global level. A corporation drafting a global privacy programme needs to anticipate an increasingly confusing and non-harmonized patchwork of legislation from jurisdictions around the world. Due to the difficulty in creating a global programme out of such a patchwork, one useful approach has been to look at how to make the different models interoperable via the development of international frameworks.

### 4- 4- Good practices

The ICT industry is not monolithic. Various hardware platforms employ diverse operating systems and applications, and users utilize an ever-increasing number of services over the internet, ranging from email to social networking, e-commerce, e-banking, e-education, etc.

Given the complexity of the ecosystem, no single ideal privacy solution exists either from a policy or a technology standpoint. Increasingly Privacy Enhancing Technologies (PETs) have been developed to protect user privacy; PETs help to increase transparency and user self-determination of their privacy rights. In this context, co-operation between government agencies, industry and organizations that provide privacy and trust services is highly desirable so as to establish good practices in the areas of both privacy and security. Such commonly agreed and sound practices would in turn reduce the risk of non-compliance as well as compliance costs for businesses by improving the predictability of the regulatory framework on privacy, in particular when it comes to its enforcement.

### 4- 5- Increased dialogue – the governance discussion

DIGITALEUROPE welcomes the efforts undertaken so far to increase the cooperation between the public and private sector stakeholders. However, there is still room for improvement. Transparency and inclusion of private sector input to the work of the Art.29 Working Party could be drastically improved; also, we welcome the opportunity to engage more frequently and openly with the Article 29 Working Party.
5- CONCLUSION

As already mentioned in the introduction to this paper, DIGITALEUROPE recognizes that there are a number of ways forward following review of the Directive: keep the status quo; complete overhaul or minor revision with selected amendments; additional specific Directives; and reinforced coordination of national approaches at European level.

Based on the above comments, DIGITALEUROPE is not suggesting that the European Commission should undertake a (major or limited) recast of the Directive. We think that the focus should be put on more harmonization, better implementation, more consistent enforcement and a move towards a more outcome-based system, rather than one merely focusing on inputs.

DIGITALEUROPE reiterates its support for the European Commission’s open consultation process between government, privacy organizations and industry on how to further improve the implementation and interpretation of the data protection framework in Europe and at a global level. We are looking forward to continuing the dialogue so as to create an environment where users can trust their use of technology, fostering technological innovation and enabling continued consumer benefits.
ABOUT DIGITALEUROPE

DIGITALEUROPE, the organisation formerly known as EICTA, is the voice of the European digital technology industry, which includes large and small companies in the Information and Communications Technology and Consumer Electronics Industry sectors. It is composed of 62 major multinational companies and 42 national associations from 29 European countries. In all, DIGITALEUROPE represents more than 10,000 companies all over Europe with more than 2 million employees and over EUR 1,000 billion in revenues.

The membership of DIGITALEUROPE

Company Members:

National Trade Associations:

Austria: FEEI; Belgium: AGORIA; Bulgaria: BAIT; Cyprus: CITEA; Czech Republic: ASE, SPIS; Denmark: DI ITEK, IT-BRANCHEN; Estonia: ITL; Finland: FFTI; France: ALLIANCE TICS, SIMAVELEC; Germany: BITKOM, ZVEI; Greece: SEPE; Hungary: IVSZ; Ireland: ICT IRELAND; Italy: ANITEC, ASSINFORM; Lithuania: INFOBALT; Netherlands: ICT OFFICE, FIAR; Poland: KIGEIT, PIIT; Portugal: AGEFE, APDC; Romania: APDETIC; Slovakia: ITAS; Slovenia: GZS; Spain: AETIC, ASIMELEC; Sweden: ALMEGA; United Kingdom: INTELLECT; Belarus: INFOPARK; Norway: ABELIA, IKT NORGE; Switzerland: SWICO; Turkey: ECID, TESID, TÜBİSİAD; Ukraine: IT UKRAINE