



## **INTEL CORPORATION<sup>1</sup> RESPONSE TO EUROPEAN COMMISSION PUBLIC CONSULTATION ON THE LEGAL FRAMEWORK FOR THE FUNDAMENTAL RIGHT TO PROTECTION OF PERSONAL DATA**

December 2009

### **A. INTEL'S GENERAL COMMENTS.**

Intel would like to thank the European Commission for launching this Consultation on "the legal framework for the fundamental right to protection of personal data". The cornerstone of this legal framework has been the European Union's ("EU") data protection directive ("the Directive"). The Directive created a binding and more harmonised framework for data protection principles in EU Member States, while at the same time improving awareness of privacy issues and serving as a reference model for other regions and countries. The Directive created a foundation of protection from which individuals could expect an environment where the individual could use technology while their right to privacy is respected.

Since the Directive's inception 13 years ago, the world has seen a dramatic evolution. We are more connected, and a global flow of data is required for today's information economy. Information technologies are providing tremendous capabilities for virtually every aspect of our lives - how we work, play, socialize, and educate. With the opportunities that accompany this new digital society also come new risks, including more sophisticated computer related threats, many of which directly affect user privacy.

These developments make it appropriate to assess the ability of the current framework and its implementation to provide effective and comprehensive protection of an individual's personal data within the EU. Fortunately, the flexible nature of the current framework provides for application to society as it develops, and we are in a position where we can deeply analyse the principles so as to best protect the rights of individuals.

Intel is of the opinion that while additional action is required to build an environment where individuals have trust and confidence in their use of technology, the core principles of the legal framework are still valid, and much can be achieved through better implementation, interpretation and communication. This document outlines Intel's response to the public consultation launched *"to obtain views on the new challenges for personal data protection in order to maintain an effective and comprehensive legal framework to protect individual's personal data within the EU"*.

Intel looks forward to continuing our engagement with the appropriate stakeholders in helping to think about ways to improve the effectiveness of the legal framework, the overall protection of privacy and increased security.

---

<sup>1</sup> Intel Corporation is a registered organisation in the European Commission's Register of Interest representatives. ID number: 7459401905-60.



## B. DETAILED CONSULTATION RESPONSE

### 1. Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation.

Intel innovates to better serve the needs of individuals by empowering them with technology that allows the control and management of different aspects of daily life. This technology creates tremendous opportunities and offers many exciting benefits, and also creates an important need to understand the implications for security and privacy. Some examples of these implications can be characterised as follows:

- **Global data flows:** given the global flow of data it is important for there to be a harmonized and predictable set of obligations across national boundaries, so that organisations can create uniform compliance policies. However, at the same time, implementation of the Directive must embrace diversity in legal, social, economic and cultural requirements. Therefore, it is important to maximise uniformity and predictability, by limiting differentiation to those situations which are absolutely necessary to reflect such differences.
- **Accountability:** accountability becomes a challenge to define as the interaction of organisations, data and technologies intermingle to support individual and global needs. More clarity and ownership of responsibility is required at all stages of the personal data life cycle, with a role for all stakeholders, including the data subjects themselves, technology designers, controllers and processors of information, and government. An optimized legal framework should encourage accountable organisations who consistently uphold the protection and rights of individuals, instead of merely seeking legal compliance.
- **Flexibility:** As complexity of processing continues to increase, stringent and detailed formal processes designed for the non-digital world sometimes reduce the ability to respond to threats quickly and to put adequate resources behind efforts that can best mitigate risk for individuals. Analysis should be made of areas where supervisory authorities can simplify existing processes (for example, notification/registrations, BCR approval), providing additional flexibility for supervisory authorities, and allowing them to prioritise resources to focus on the largest risks.
- **Law Enforcement:** the separation between data processed solely by private entities and that which is accessed by law enforcement and government intelligence agencies has substantially eroded. Access by law enforcement to personal data held by private entities can take place in different ways, such as via legal process or where governments act as commercial actors and purchase data. Following the entry into force of the Lisbon Treaty, the EU Commission, the EU member states and the European Parliament now have the opportunity to analyze the impact of law enforcement processing of personal data obtained from the private sector. However, such analysis will need to be deliberate and fully understand the impact to government, private sector and individuals. This analysis must also determine the proper framework for application of the principles, while improving transparency of personal data processing for law enforcement purposes.



## **2. In your views, (does) the current legal framework meet these challenges?**

The European legal framework for the protection of personal data has stood the test of time remarkably well. While there are issues of interpretation, implementation and communication, the overall principles remain valid.

- The globally recognized framework of compliance principles and rules provide for individual rights and important concepts such as transparency, proportionality, accountability, minimisation, security, access, choice and control.
- The role of a Personal Data Protection Official<sup>2</sup> (“DPO”) provides a vehicle for credible independent expertise and oversight, when backed by proper organisational governance, enforcement and accountability. DPOs understand business processes and data flows and can influence their design in ways that best protect the rights of individuals. The nurturing of the growing privacy profession has the potential to greatly increase the degree to which individuals’ rights are respected.
- Maintaining technology neutrality in the legal framework provides protection for individuals in a rapidly evolving technological society. The creation of legislative and regulatory requirements will invariably trail innovation of new technology. Therefore, a focus in the application of principles, neutral to the technology used, enables a flexible, effective and timely response.
- Exploration of the concept of the definition of personal data has proven that the interpretation, implementation and communication of the Directive for meaningful application to daily life is possible within the current framework. Additional enhancements to aid the consistent interpretation of this and other provisions of the Directive must be explored by the Commission, such as greater efficiency in the process of bringing together supervisory authorities, and the official ratification of harmonised interpretations.

---

<sup>2</sup> Directive 95/46/EC Chapter II, Section IX, Article 18



In light of the new challenges presented by today's complex data protection and privacy environment, certain areas within the current legal framework should become focus areas for improvement through better interpretation, implementation and communication:

- **International data transfers** have grown in complexity, while lacking a practical mechanism for compliance, and a culture of accountability for organisations of all types and sizes. So long as an organisation of any size provides adequate protection and accountability, transfers of personal data should take place without need for complex, lengthy and costly administrative processes. Adequate protection should not be interpreted as equivalency to the Directive, but instead should focus on whether the core principles of the Directive are met. A short or medium term resolution for large organisations transferring data internationally has been achieved with the creation and implementation of the Binding Corporate Rules (BCRs) approvals process. Further work is required to simplify the processes for drafting and ratifying BCRs and to encourage organisations to adopt them, in the recognition that implementation of such internal accountability measures does provide real protection for individuals.
- **Notification** fulfils an important and positive purpose for transparency and accountability, yet the approval and prior checking of personal data processing has become overly cumbersome and bureaucratic in many countries. Notification and registration should be greatly simplified to focus on providing the contact points (for example a DPO), education and enforcement. Insufficient use has been made of the opportunity to recognise DPO appointments (with a potential scope of responsibility for one or multiple countries) as an effective compliance measure, and to provide an exemption from all detailed registration and notification requirements, including situations where data is transferred internationally.



### 3. What future action would be needed to address the identified challenges?

In order to address the challenges outlined in the responses to the previous two questions, Intel would propose that future action be divided into four distinct efforts:

- i. **Harmonisation** efforts within the EU must continue to focus on consistent implementation and interpretation to ensure effective privacy protection for global information processing while respecting the sensitivities of local environments. The need for individual member states to be able to customize their legislation to take into account certain unique legal, social, economic and cultural differences should be recognised. However, greater focus is required on limiting member state specific customisation of the legal framework, in order to provide greater clarity of individual rights, and to simplify the implementation of operational measures. For example, there are good reasons for member states to define sensitive data in different ways depending upon their culture. However, there is less justification for widely varying requirements for providing access to personal data, especially given the impact such varying access requirements can make on organisations designing global processes to protect individuals privacy rights. European authorities should work together to provide harmonised guidance to organisations which collect and process personal data. The development of non-governmental organisations (“NGOs”) can contribute to this harmonisation by working in partnership with supervisory authorities and other key stakeholders to recommend best practices. Moreover, harmonised and predictable enforcement will ensure that responsible organisations are not at a disadvantage compared to those which refuse to invest in processes that respect the rights of individuals.
- ii. **Accountability** is a principle found in many instruments of the legal framework<sup>3</sup>, and which has been summarised as *“the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations”* and as going *“beyond responsibility by obligating an organisation to be answerable for its actions.”*<sup>4</sup> The respect for the right of privacy is only realised if organisations invest in processes to drive accountability when processing personal information. This investment in processes designs privacy into the organisation, so that data protection becomes a proactive part of the business, instead of a reactive compliance function. The Directive provides the basic tools through which member state authorities can encourage an accountability system, but these tools must be used in a more coherent, harmonised and predictable fashion. For example:
  - a) DPO appointments should be encouraged by allowing organisations which have made such an appointment to only register or notify the contact details of the DPO, even in situations involving the international transfer of personal data.

---

<sup>3</sup> For example: Directive 95/46/EC; Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Asia Pacific Economic Cooperation (APEC) Privacy Framework; Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA); USA’s Safeguards Rule of the Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley Act)

<sup>4</sup> “Data Protection Accountability: The Essential Elements A Document for Discussion” from the Center for Information Policy Leadership (CIPL) - October 2009



- b) The DPO provisions in the Directive could be implemented in a way to require the supervisory authorities to empower the DPO, and to assist by fostering professional organisations that help to educate and connect the DPO with the growing global privacy profession. DPO outreach and education should be further prioritised, and should include provision of approved curriculum and certifications focussed on mastery of how to protect personal data.
- c) Investment should be made in working with NGOs which focus on the development of the privacy profession and which can help assist DPOs in the implementation of effective privacy compliance programs.
- d) BCRs can function within an organisation as a foundation of accountability by making compliance expectations clear, as well as the penalties of non-compliance. However, the BCR drafting and approval process must be further simplified. The approval process should include true mutual recognition where one approval represents all.
- e) Designing in privacy is a foundational component of accountability, and the Directive currently provides the necessary structure to encourage such integration of privacy principles into corporate and government processes. Supervisory authorities should look for mechanisms that encourage organisations to incorporate privacy by design processes. These mechanisms should be focused on the outcomes rather than prescriptive procedures and should look at how to positively incentivize organisations. For example, DPO education can be used to promote the benefits of the incorporation of the flexible principles of the Directive into product and program development processes, and privacy impact assessments. As long as these principles remain technology neutral and sufficiently flexible, they can assist those who are creating new programs, products and services to understand how to accomplish their business goals while also protecting individuals' privacy rights.
- f) Harmonized, predictable and robust enforcement must be conducted to make certain that organisations which do not invest in processes to protect personal data are held to account. Enforcement activity should be signalled ahead of time, focussed on clearly defined unacceptable practices, and the results should be communicated globally to reinforce accountability, making clear the risks of bad practices. Supervisory authorities should collectively analyze different frameworks which could provide such predictable harmonized enforcement.



**iii. Best practices** are linked to the principle of accountability. An accountable organisation protects information in a manner consistent with agreed upon expectations set out in, amongst other things, best practices. These can be a useful tool for supervisory authorities to help interpret the high level principles of the Directive.

Best practices development initiatives have greater flexibility in approach and allow for faster response to new methods of processing personal data. They can also provide consistency of approach internationally, enabling government and company resources to focus on implementation rather than interpretation. Such development must focus on individual rights, and include input from those who are close to understanding data flows and operational practices. Moreover, best practices have an important role to play in the facilitation of awareness and understanding, for example in setting the expectations of individuals by establishing a baseline that provides precedent and transparency, or as a tool to help educate the supervisory authorities on what should be considered as reasonable for different size organisations in providing security for personal data.

Examples of areas for improvement that could be addressed by the development of best practices are:

- data subject access requests (creating a baseline while avoiding the exploitation of rights for inappropriate “fishing expeditions”),
- better guidance on effective notice to individuals,
- guidance on implied consent (for example when ordering a book online, does the individual implicitly consent to the transfer of delivery information to the shipping company?),
- template BCRs for different organisations to use as starting points in the drafting process,
- security and threat protection that keeps pace with the rapid evolution of personal data processing technologies and processes.

EU and member state authorities should provide substantive input to the development of these best practices by creating working relationships with NGOs, professional associations, or other organisations that can help by developing best practices for privacy and security. The Commission should explore the possibility of continuing Framework Program funding for organisations that develop best practices.

**iv. Awareness and Education** is not obligatory, yet is universally recognised as a key component for provision of understanding and protection of fundamental rights. Several supervisory authorities have led by example in working together with other stakeholders in raising such awareness about the risks from privacy invasions, and how to protect oneself, exercise rights, or lodge claims<sup>5</sup>. However, more consistent investment in coordinated programs is required, as well as additional focus on educating individuals and those processing personal data. This could be accomplished by providing support for civil society, NGOs,

---

<sup>5</sup> An example of such cooperation are the annual Data Protection Day activities, where stakeholders work together to raise awareness.



professional associations and other organisations who have privacy awareness and education as their primary mission, and regularly report on their progress to the general public.

## C. CONCLUSION

The European legal framework for the fundamental right to protection of personal data provides a globally-recognised reference model. In order to continue to provide world leadership in the constantly evolving data protection and privacy environment, constant review and refresh of interpretation, implementation and communication of the legal framework are essential.

To summarise, Intel is pleased to have the opportunity to offer these recommendations for consideration in this consultation process:

- **Harmonisation** efforts are required for the continued success of the European legal framework for the fundamental right to protection of personal data. This can be achieved with greater guidance at the European level, and with reduced legal framework customisation at member state level.
- **Accountability** must be a prerequisite for personal data use. It should embrace compliance and enforcement driven by regulation and concept definitions. It should also take into account privacy by design, better leverage of the DPO role, as well as best practices drawn from the “Triangle of Trust” made up by companies, government organisations and NGOs.
- **Best Practices**, Codes of Conduct created with input from a range of stakeholders including supervisory authorities, companies, NGOs, professional associations, or other organisations, should be used to drive flexible and consistent improvements that keep pace with the rapid evolution of personal data processing technologies and processes.
- **Awareness and Education** should become more coordinated, available and visible for all those involved in the processing of personal data, driven collaboratively by companies, EU institutions, civil society, NGOs and supervisory authorities.

Intel looks forward to continued engagement with all relevant stakeholders in helping to think about ways to improve the effectiveness of the legal framework for the fundamental right to protection of personal data, and of overall protection of privacy and increased security.

### About Intel

For decades, Intel Corporation has developed technology enabling the computer and Internet revolution that has changed the world. Founded in 1968 to build semiconductor memory products, Intel introduced the world's first microprocessor in 1971. Today, Intel the world's largest chip maker is also a leading manufacturer of computer, networking, and communications products. For more information see <http://www.intel.com>