Key points on the Proposed EU Data Protection Regulation

Summary

Technologies are providing tremendous capabilities for virtually every aspect of our lives: how we play, work, socialize, and educate. We are more connected than ever, and a global flow of data is required for today's information economy. Given these technological changes and the increase of cross border data flows, Intel agrees it is appropriate to update the current Data Protection Directive. We therefore welcome the intent of the European Commission's proposed Regulation as it aims to strengthen the individual's rights and at the same time recognizes the importance of cross border data flows.

However, we believe certain areas need to be further clarified and strengthened for the Regulation to achieve these objectives;

- First, we need to ensure that the Regulation will stand the test of time. The key to achieving this is for the Regulation **to remain technology neutral**. Intel therefore proposes to insert specific language into the Regulation on technology neutrality which would highlight it as a guiding principle of the Regulation.
- **Security is key to protecting user's data and networks:** with the opportunities that accompany the new digital era also come new challenges. These challenges include more sophisticated computer related threats, many of which directly affect user privacy. Intel welcomes the proposed Regulation's strong focus on the need for security measures being put in place to protect user's data and networks. But it is critical for organizations and their providers of security technologies and services that there is more legal certainty on the legitimate ground for processing data where this is needed to implement such security measures. Inserting a new paragraph in art. 30 reflecting the language of recital 39 would ensure that users' data and networks can continue to be protected. At the same time, we also propose some slight modifications to the breach notification requirements to make it more efficient.
- **Focus on outcome instead of means – towards a workable Regulation:** Intel agrees with the Commission on the need to strengthen organizations' responsibility, or, as we refer to it, "accountability." A true accountability approach moves from an *ex-ante* to an *ex-post* model, setting the objectives and potential ways to achieve those objectives. However the current provisions outlined in the Regulation are too detailed and prescriptive, and risk increasing administrative burdens without any commensurate increase of data protection.

Introduction

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 is the world's largest chip maker and a leading manufacturer of computer, networking, and communications products. We provide the building blocks for a spectrum of devices which we call the *"*Compute Continuum*"* (the interconnectedness of PCs, laptops, tablets, smartphones, televisions, etc.). The use of these connected devices, and the numerous applications which run on them is transforming the way we work, socialize, and play. However, along with these benefits come concerns about privacy and security.

Why does Intel care about Privacy and Security?

For people to continue using these devices and future innovative technologies, trust is required. Intel has recognized for years that privacy and security are two interrelated components which can increase trust. If consumers and businesses do not trust that their online information is private and secure, then they will buy fewer products, negatively affecting growth of the e-commerce and telecommunications sector.[1] Intel believes the best way to ensure this trust is through the adoption of efficient, technology neutral, and harmonized legislation.

Strong security enables strong data protection

Privacy and security are crucially interrelated. Strong security is needed to protect private information. **We welcome the European Commission's proposal for a specific chapter on security** which highlights the interrelationship and which stresses the need for organizations to implement measures to protect data and which includes a data breach notification regime. In addition to this, recital 39 recognizes the need for more legal certainty with regards to the lawfulness of processing of data for exactly such purposes.

Making the Regulation more efficient

Intel welcomes the European Commission's goal of having a more efficient legislative framework by reducing the unnecessary administrative burdens, such as the elimination of notification obligations. Removal of such administrative burdens has the potential to result in more effective privacy protection as organizations can focus resources on managing personal data appropriately, instead of focusing those resources on processing paperwork. However, the Regulation **introduces several new and substantial administrative obligations** that are not narrowly tailored and for which there is no indication they will increase privacy protection for the data subject. These obligations will make the **regulation less efficient and less effective**, undermining the stated objective by the European Commission to reduce such burdens.

[1] An additional important component of trust is awareness. Intel has been a strong supporter of increased awareness raising activities such as, but not limited to, the annual Data Protection/Privacy Day on January 28th. Any legislative effort should also recognize the importance of awareness.

Suggested changes to the Regulation

1. Technology Neutrality

One of the biggest achievements of the current Data Protection Directive has been **its technology neutral characte**r, with the absence of detailed rules which would mandate or otherwise compel adoption of any one specific technology. This technology neutral approach allows engineers to do what they do best: solve problems. By describing neutral principles and objectives, global innovators can collaborate on the best way to implement solutions. This approach has enabled the Directive to stay in force for over 15 years and this will also need to be the case for the Regulation if it too wants to withstand the test of time.

As Commissioner Reding said, "We can only imagine how technology will change our lives tomorrow. That is why the new regulatory environment has to be future-proof, be technology-neutral."[2] Therefore Intel would like to propose this principle be mentioned in recital 13, again, at the start of the Regulation as a signal of its importance as an underpinning principle and this within article 2**.**

We also think that a reflection of this principle within the context of the delegated acts should be added in art. 86.6 (new) to ensure that any decision as a follow up act is taken in line with this principle.

2. More legal certainty is needed for organizations that protect personal data via strong security

Consumers are increasingly concerned about the security of their online information and desire their information to be protected. The results of the latest Eurostat survey on the information society showed that "around half (49%) of all internet users reported having at least once avoided an activity on the internet due to security concerns; the most common of these was to avoid providing personal information on social networking sites, followed by e-commerce (buying goods or services over the internet) and e-banking."[3] To ensure greater trust and security online, Intel strongly welcomes the provisions in the Regulation's **section on data security (art. 30)** which require organizations to have technical and organizational measures in place to protect personal data. However, organizations themselves or the security technology providers they rely on often need to process data for stronger security. In most cases this data is not personal data. In those instances where it would be considered personal data, the right safeguards will need to be in place as with all processing of personal data falling within the scope of the Regulation.

The current legal framework needs to clarify that processing of data for such security purposes, constitutes a legitimate interest of the concerned organization. This already has been recognized by the European Commission in the current language within **recital 39** but given its importance for protecting users' data and the security of networks, Intel is of the opinion that the language of recital 39 should be reflected in the body of the Regulation.

---

[2] Speech on the *EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World*, delivered by Vice President Reding on 25 January 2012

[3] Information Society Statistics, Eurostat, September 2011

Failure to reflect the need for processing for stronger security within the body of the text of the Regulation **will create legal uncertainty** which malicious actors could exploit. If we want to avoid this and enable a more secure online environment for users, an explicit recognition of the fact that processing for stronger security constitutes a legitimate interest will be required.

We also think the current recital 39 and the above mentioned changes should not only focus on **the data controller** but also the **processor,** as some organizations will hire external organizations such as McAfee to put in place those security measures.

3. Towards a workable data breach notification obligation

Intel agrees that the **scope** of a notification system should only encompass *personal* data breaches, and not move beyond this. With regards to **thresholds**, as outlined currently in art. 32, data subjects should only be notified when a breach is "likely to adversely affect the protection of the personal data or privacy of the data subject." We believe the same standard should be applied in the requirement to notify the supervisory authority in art. 31.1.

Under art 32.3, an organization is not required to notify the data subject **when technological protection measures** are put in place. We would like to propose the same approach is adopted in art. 31 on notifications to supervisory authorities. We believe that as these breaches would still need to be documented, as outlined in art. 31.4, supervisory authorities can always hold organizations accountable with regards to their potential non – actions.

The **timing** of reporting material breaches to the supervisory authorities should be flexible so as not to interrupt the organization's efforts to deal with a breach event. Therefore, we propose that the 24 hour rule be removed as this will only result in a range of notifications during a period where even the organizations themselves may not yet be sure of what exactly happened. We propose to maintain the "without undue delay" provision which would bring it in line with art. 31.

4. A more efficient data protection framework

The Regulation proposes new requirements which are framed in such a way that they increase administrative burdens without guaranteeing strong additional benefits for data protection. One example of such a requirement is the **broad documentation obligation** that requires "all processing operations" to be documented by an organization. This obligation is not well defined and risks creating unnecessary and overly detailed paper trails which could impose substantial costs with no commensurate benefit to data subjects. Instead of focusing on creating paperwork, we recommend the Regulation concern itself with outcomes. Therefore, we propose to more narrowly target the obligation in art. 28 to document to "the main categories of processing" and to only require controllers and processors to list "generic purposes of processing."

Another example is the broad requirement for **Data Protection Impact Assessments (DPIAs)**. DPIAs are a useful tool as part of accountability measures and they are most effectively implemented when they allow flexibility for an organization to tailor the assessment to their particular organization and business processes. Mandating prescriptive DPIAs could run counter to the many different methods organizations across the globe have to assess privacy (and security) impacts, we therefore propose to remove the delegated and implementing acts of the European Commission in paragraphs 6 and 7 of art. 33 and the detailed requirements on the content of PIAs in paragraph 3.

Given that the DPIAs can contain sensitive information about product developments, organizations **should not be required to make these public and request feedback from data subjects** as outlined in paragraph 4. This requirement will slow down development while not bringing any clarity as to what the added benefit would be for the data subjects.

The Regulation should not create the burden of **mandating companies to turn over on a constant basis the DPIAs to the supervisory authorities** as outlined in article 34.6. Any such requirement to provide the DPIAs in a proactive manner runs the risk of the legal staff treating every DPIA as a potential regulatory filing. This could lead to delay in the review process, and impede the ability of the privacy compliance staff to effectively design in privacy at the earliest stages in product/service/program development. The possibility for the supervisory authorities to request access to specific DPIAs will provide enough guarantees for review. It should also be noted that the proposed system will significantly strain the supervisory authorities' resources without adding any strong increase in data protection.

Finally, the possibility for supervisory authorities to **draw up additional list of specific risks**, will create opportunity for confusion and divergent approaches across the EU. This runs counter to the goal of a stronger harmonization. We therefore propose to remove paragraph 2 (e) and the relevant provisions in article 34.

Conclusion

Intel would like to thank you for considering our concerns and proposals. We look forward to continuing our engagement with all stakeholders and ensuring that the Regulation will be a future-proof legislative framework.

Christoph Luykx
Privacy and Security Policy manager for Europe
Global Public Policy, Intel Corporation
Rue Froissart 95, 1040 Brussels
+32 (0) 2 545 1912
+32 (0) 47 3 786 447
christoph.luykx@intel.com