72

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 16:01
To: Verweij, Ellen
Subject: FW: Intel Corporation ontmoeting data protection
Attachments: Intel Corporation key points on Data Protection Regulation.pdf; Intel Corporation Proposed Amendments Data Protection Regulation.pdf

Follow Up Flag: Follow up
Flag Status: Completed

From: [redacted] [mailto:[redacted]
Sent: woensdag 12 december 2012 18:38
To: Kaai, Geran
Cc: [redacted]
Subject: Intel Corporation ontmoeting data protection

Geachte heer Kaai,
Beste Geran,

Nogmaals bedankt voor de ontmoeting van vandaag. Ik stuur u in bijlage de documenten die we besproken hebben tijdens ons onderhoud.

Bij deze wens ik u alvast prettige feestdagen en hoop u snel opnieuw te mogen ontmoeten.

Met vriendelijke groeten,

[redacted]

[redacted]
Public Policy Manager
Intel Corporation
95 Rue Froissart
1040 Brussels
T+[redacted]
M+[redacted]
[redacted]
www.intel.eu
Intel public policy blog: http://blogs.intel.com/policy

Follow us on Twitter: @Intel_EU

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 character**, 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.

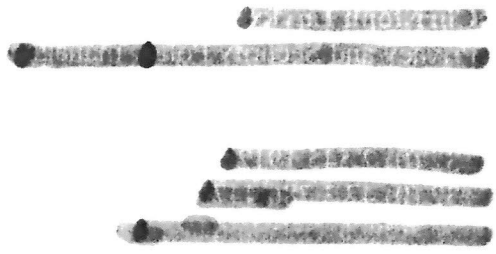
The Regulation should not create the burden of **mandating companies to turn over on a constant basis the DPIAs to the supervisory authorities** as outlined in article 34.6. Any such requirement to provide the DPIAs in a proactive manner runs the risk of the legal staff treating every DPIA as a potential 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.

[redacted] for Europe
Global Public Policy, Intel Corporation
Rue Froissart 95, 1040 Brussels
[redacted]



OVERVIEW OF PROPOSED AMENDMENTS

1. **Technology neutrality (art 2 and art 86)**
2. **(Lawfulness of processing for security purposes (R 36, R 39, art 6 (1)c, 6(1)f, and R66, art 30.3, art 30.3 (new) and 30.4)**
3. **Data breach notification (art 31)**
4. **Administrative requirements (art 28, 33 and 34)**

Technology neutrality

Amendment 1
Proposal for a regulation
Article 2

Text proposed by the Commission	*Amendment*
1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing	1. This Regulation applies to the processing of personal data wholly or partly by automated means, ***without discrimination between such processing means***, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing.

Amendment 2
Proposal for a regulation
Article 86

Text proposed by the Commission	*Amendment*
	6 (new) ***Acts adopted in accordance with this Article shall be technology neutral and non-discriminatory irrespective of the means used for the lawful processing of personal data.***

Justification

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level - technologically neutral and future proof for the decades to come. The protection of individuals should be technologically neutral and not depend on the means or technologies used for such processing.

Lawfulness of processing **R 36, R 39, art 6 (1) c, 6 (1) f, and R 66, article 30.3 (new) and 30.4**

Amendment 3
Proposal for a regulation
Recital 36

Text proposed by the Commission	*Amendment*
(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.	(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject, ***including the obligation to implement appropriate technical and organisational measures to ensure the security of processing pursuant to Article 30 of this Regulation,*** or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.

Justification

A reference to the provisions on the security of data processing (Articles 30 and following) clarifies that the obligations created under this Regulation to protect personal data against accidental or unlawful destruction, accidental loss or to prevent any unlawful forms of processing constitute a legal obligation pursuant to Article 6 paragraph 1 c.

Amendment 4
Proposal for a regulation
Recital 39

Text proposed by the Commission	*Amendment*
(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams ¬ CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.	(39) The processing of data ***by, or on behalf of, a controller, or a processor*** to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest ~~**of the concerned data controller.**~~ This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Or. en

Justification

In the information society, data privacy cannot be guaranteed without the implementation of technical and organisational security measures by, or on behalf of a data controller or processor. To maintain network and information security and protect the users' terminals, it may be the case that in specific cases personal data need to be processed. Such processing constitutes a legitimate interest of the controller under Article 6 paragraph 1 f and in line with Recital 39.
As an illustration of the critical importance of processing data to ensure network and information security, in a recent response to question E-007574/2012 by MEP Marc Tarabella (S&D), the EU Commission acknowledges that it already has "duty to take all the

necessary measures to ensure a high rate of availability of its websites for all citizens (and those it manages for other institutions) against (cyber-) attacks". In this case, the EU Commission acknowledges that it is blocking access to its website for users of TOR (The Onion Router) as it considers these measures "necessary to mitigate risks and counteract attacks that occur, taking account of the technical specificities of the latter".

Amendment 5
Proposal for a regulation
Article 6 – paragraph 1– point c

Text proposed by the Commission	*Amendment*
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject, ***including for the security of processing subject to the conditions and safeguards referred to in Article 30;***

Or. en

Justification

An explicit reference to the provisions on the security of data processing and the conditions and safeguards referred to in Articles 30 is required to clarify that the security of processing is a legal obligation created under this Regulation which requires processing to take place in order to protect personal data against accidental or unlawful destruction, accidental loss and to prevent any unlawful forms of processing.

In the information society, data privacy cannot be guaranteed without the implementation of technical and organisational security measures that may require the processing of data. A practical example of such measures is the blocking of certain IP numbers by the EU Commission for security purposes, as illustrated in its response to question E-007574/2012 by MEP Marc Tarabella. In this case, the duty of the Commission includes the processing and blocking access of to its public websites for certain IP numbers associated with the TOR online anonymizer.

Amendment 6
Proposal for a regulation
Article 6 – paragraph 1 – point f

Text proposed by the Commission	*Amendment*
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	(f) processing is necessary for the purposes of the legitimate interests pursued by, ***or on behalf of,*** a controller ***or a processor, including for the security of processing,*** except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Or. en

Justification

A specific reference to the provisions on the security of data processing (Articles 30 and following) clarifies that the processing of data to the extent strictly necessary for the purposes of ensuring network and information security by, or on behalf of, a data controller, or data processor constitutes a legitimate interest of the concerned data controller or of the processor. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Amendment 7
Proposal for a regulation
Recital 66

Text proposed by the Commission	*Amendment*
(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and	(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. ***When the implementation of such measures***

organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.	***requires processing of data to increase network and information security, such processing constitutes a legitimate interest pursued by, or on behalf of the controller or the processor.*** When providing guidance on ~~**establishing technical standards and**~~ organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.

Or. en

Justification

Data controllers and processors should ensure that they have the right organizational measures in place to ensure security of processing and hence, enhancing overall network and information security. Where the implementation of such measures would require the processing of data to the extent strictly necessary for purposes of ensuring network and information security by the data controller or the processor, such processing should be deemed to be a legitimate interest for processing in line with recital 39 and Article 6(1) (f). A practical example of such measures is the blocking of certain IP numbers by the EU Commission, as illustrated in its response to question E-007574/2012 by MEP Marc Tarabella

Amendment 8
Proposal for a regulation
Article 30 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default,	~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default,~~

unless paragraph 4 applies.	~~unless paragraph 4 applies.~~

Or. en

Justification

Considering the pace of innovation and the aim of creating a modern horizontal data protection framework that is technologically neutral, future-proof results cannot be achieved if the technical 'state of the art' is defined by means of delegated acts for each individual sector. Imposing sector-specific technical requirements or mandates and defining the 'state of the art' by means of delegated acts is unlikely to keep up with the pace innovation and is in direct contradiction with the technology neutrality goal pursued by this Regulation.

Or. en

Amendment 9
Proposal for a regulation
Article 30 – paragraph 3 (new)

Text proposed by the Commission	*Amendment*
	3. The legal obligations, as referred to in paragraphs 1 and 2, which would require processing of personal data to the extent strictly necessary for the purposes of ensuring network and information security, constitute a legitimate interest pursued by, or on behalf of a data controller or processor pursuant to Article 6 paragraph 1 f .

Or. en

Justification

Data controllers and processors should ensure that they have the right organizational measures in place to ensure security of processing and hence, enhancing overall network and information security. Where the implementation of such measures would require the processing of data to ensure network and information security by the data controller or the processor, such processing should be deemed to be a legitimate interest for processing in line with recital 39 and Article 6(1) (f). A practical example of such measures is the blocking of certain IP numbers by the EU Commission for security purposes, as illustrated in its response to question E-007574/2012 by MEP Marc Tarabella

Amendment 10
Proposal for a regulation
Article 30 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:	~~*4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:*~~
(a) prevent any unauthorised access to personal data;	~~*(a) prevent any unauthorised access to personal data;*~~
(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;	~~*(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;*~~
(c) ensure the verification of the lawfulness of processing operations.	~~*(c) ensure the verification of the lawfulness of processing operations.*~~
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~*Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Or. en

Justification

Considering the pace of innovation and the aim of creating a modern horizontal data protection framework that ensures a high level of protection within the European Union but also at international level, technical standards with respect to organisational measures to ensure security of processing should not be adopted by the European Commission by way of implementing acts but should rather be developed at a more global level.

Breach notification (article 31)

Amendment 11
Proposal for a regulation
Article 31

Text proposed by the Commission	*Amendment*
Notification of a personal data breach to the supervisory authority	Notification of a personal data breach to the supervisory authority
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.	1. In the case of a personal data breach ***that is likely to adversely affect the protection of the personal data or privacy of the data subject***, the controller shall without undue delay ~~***and, where feasible, not later than 24 hours***~~ after having become aware of it~~,~~ notify the personal data breach to the supervisory authority. ~~***The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.***~~ ***The notification of a personal data breach to the supervisory authority shall not be required if the controller has implemented appropriate technological protection measures, and those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.***
2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.	2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach
3. The notification referred to in paragraph 1 must at least:	***3. To the extent feasible given the timing of the notification and the***

	circumstances of the personal data breach, ~~*T*~~the notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including the categories and ***approximate*** number of data subjects concerned and the categories ~~***and number***~~ of data records concerned;
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	***(c) include any*** recommend***ed*** measures ***for the data subject*** to mitigate the possible adverse effects of the personal data breach;
(d) describe the consequences of the personal data breach;	~~***(d) describe the consequences of the personal data breach;***~~
(e) describe the measures proposed or taken by the controller to address the personal data breach.	(e) describe the measures ~~***proposed or taken***~~ ***that have been or will be implemented*** by the controller to address the personal data breach ***and to mitigate its possible adverse effects***.
4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must ***be sufficient to*** enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.	~~***5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.***~~
6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	6. The Commission may ***recommend*** ~~***lay down the***~~ ***a*** standard format ***which controllers may choose to use for*** ~~***of***~~ such notification to the supervisory authority, ***and*** the procedures applicable to the ***filing of reports.*** ~~***notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein.***~~ Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

As outlined currently in art. 32, data subjects should only be notified when a breach is "likely to adversely affect the personal data or privacy of the data subject." By including this reflection of the same harm standard in the requirement to notify the supervisory authority in art. 31 (1), the overall consistency of the system will be improved and it will also avoid over notifications to the Supervisory Authorities, hence allowing the latter to focus on those cases where there has been an impact to the personal data or privacy of the data subject.

According also to art. 32, an organization is not required to notify the data subject when technological protection measures are put in place by the organisation that render the data unintelligible to any person who is not authorised to access it. The same provisions should be reflected in art. 31 which would specify that a notification to a supervisory authority is not required where such measures are in place. 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 in case of non – action and at the same time ensures a more workable notification system focusing on those instances where harm is caused.

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. The organization's efforts to remedy the breach should not be diluted by the need to shift resources to notifying the supervisory authority. Therefore, we propose for the 24 hour rule to be removed as this will only result in a whole range of notifications even though the organizations are not sure what exactly happened. We propose to maintain the "without undue delay" provision which

would bring it in line with art. 31.

The delegated acts for the European Commission should be deleted but we propose to maintain the implementing act for potential standard voluntary notification forms and determining the procedures as this might ensure some more harmonisation in the notification requirement.

Administrative requirements (28, 33 and 34)

Amendment 12
Proposal for a regulation
Article 28 (documentation)

Text proposed by the Commission	*Amendment*
1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of ~~***all***~~ ***the main categories of*** processing operations-under its responsibility.
2. The documentation shall contain at least the following information:	2. The documentation shall contain at least the following information:
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
(b) the name and contact details of the data protection officer, if any;	(b) the name and contact details of the data protection officer, if any;
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	(c) the ***generic*** purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(d) a description of categories of data subjects and of the categories of personal data relating to them;	(d) a description of categories of data subjects and of the categories of personal data relating to them;
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;	(e) the ~~***recipients or***~~ categories of recipients of the personal data. ~~***,including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;***~~
(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	(f) where applicable, transfers of ***personal*** data to a third country or an international organisation~~***, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), a reference to the documentation of appropriate safeguards employed;***~~

(g) a general indication of the time limits for erasure of the different categories of data;	(g) a general indication of the time limits for erasure ***or data retention policy applicable to*** ~~***of***~~ the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).	(h) the description of the mechanisms referred to in Article 22(3).
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on the basis of a request outlining the reasons for requiring access to the documents, to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:	4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:
(a) a natural person processing personal data without a commercial interest; or	(a) a natural person processing personal data without a commercial interest; or
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.	5~~***. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.***~~
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	6. The Commission may recommend ~~***lay down***~~ ***non mandatory*** standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Effective data protection requires that organisations have sufficiently documented understanding of their data processing activities. Instead of satisfying bureaucratic needs, the aim of the documentation should be to help controllers and processors meet their obligations.

Companies have many ways of documenting their data processing environment and no specific method should be mandated. Often such documentation exists through multiple means. A very detailed documentation procedure would remain an almost instantly outdated snapshot of a constantly changing reality characterized by complex data processing arrangements in a multiparty environment. Therefore, the documentation obligations should focus on outlining the main categories of processing operations instead of all detailed processing and the delegated acts for the European Commission should be deleted. The implementing act to develop non-mandatory standard forms for documentation requirement should be maintained.

Amendment 13
Proposal for a regulation
Article 33 (Data Protection Impact Assessment)

Text proposed by the Commission	*Amendment*
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1:	2. The following processing operations in particular present specific risks referred to in paragraph 1:
(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;	(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, ~~**location**~~, health, personal preferences, reliability or behavior, which is based on automated processing and on which measures are based that produce legal effects ~~***concerning the individual or significantly***~~ ***that gravely and adversely*** affect the individual***'s fundamental rights;***
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or	(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for

decisions regarding specific individuals on a large scale;	taking measures or decisions regarding specific individuals on a large scale;
(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;	(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;
(d) personal data in large scale filing systems on children, genetic data or biometric data;	(d) personal data in large scale filing systems on children, genetic data or biometric data;
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).	~~*(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).*~~
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.	~~*3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.*~~
3. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	~~*4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.*~~
4.	
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing	5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing

operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.	operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	~~*6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.*~~
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~*7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Justification

Data Protection Impact Assessments (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 and the detailed requirements on the content of PIAs in paragraph 3.

Given that the DPIAs can contain sensitive information with regards to product developments, organizations should not be required to make these public and request feedback from data subjects as outlined in par 4. Such a requirement will slow down development and it is also not clear what the added benefit would be for data subjects. The possibility for the supervisory authorities to request access to DPIAs should provide enough guarantees.

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 pro-active manner, will likely result in the legal staff treating every DPIA as a potential regulatory filing. This consideration of legal risk has the

potential to create 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 sufficient guarantees for review.

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 which runs counter to the goal of a stronger harmonization. We therefore propose to remove paragraph 2 (e) and the relevant provisions in article 34.

Amendment 14
Proposal for a regulation
Article 34 (Prior Authorisation and Prior Consultation)

Text proposed by the Commission	*Amendment*
1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.	1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.
2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:	2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to	(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely

present a high degree of specific risks; or	to present a high degree of specific risks; or
(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	~~*(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.*~~
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.	3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.
4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	~~*4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.*~~
5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.	~~*5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.*~~
6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in	**6.** The controller or processor shall, ***on request***, provide the supervisory authority with the data protection impact assessment provided for in Article 33 and~~,~~ on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the

particular of the risks for the protection of personal data of the data subject and of the related safeguards.	processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.
7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.	~~***8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.***~~
9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	9. The Commission may set out ***non mandatory*** standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

The possibility for supervisory authorities to draw up additional list of specific risks, will create opportunity for confusion and divergent approaches across the EU which runs counter to the goal of a stronger harmonization. We therefore propose to remove paragraphs 2 (e), 4 and 5. 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 pro-active manner, will likely result in the legal staff treating every DPIA as a potential regulatory filing. This consideration of legal risk has the potential to create 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. We therefore propose to add "on request" to the language in article 34 (6). We also propose to remove the delegated acts for the European Commission.