Intel

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)**

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.

Intel

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.

Intel

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	(f) processing is necessary for the purposes of the legitimate interests pursued by, ***or***

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.	***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 organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.	(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 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, unless paragraph 4 applies.	***Deleted***

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.

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:	***Deleted***
(a) prevent any unauthorised access to 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.	
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.