AmCham EU Proposed Amendments on the General Data Protection Regulation

CONTENTS

1. Consent and profiling

Proposal for a regulation
Recital 25

Text proposed by the Commission	*AmCham EU Amendment*
(25) Consent should be given ***explicitly*** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. ***Silence or inactivity should therefore not constitute consent***. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	(25) Consent should be given by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Justification

The imposition of "explicit" consent in every circumstance is not compatible with the notion that a request "must not be unnecessarily disruptive to the use of the service for which it is provided". The economic consequences of such a paradigm shift – which would fundamentally change the nature of internet users' relationship with the internet - need much greater investigation. Ruling out implied or tacit consent will encourage data controllers to authenticate users, increasing the amount of personal data held rather than reducing it. Explicit consent should be reserved for sensitive categories of data.

Proposal for a regulation
Recital 33

Text proposed by the Commission	*AmCham EU Amendment*
(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent ***without detriment***.	(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent.

Justification

The concept of "without detriment" places an excessive burden on the organization from whom consent is withdrawn. Organisations should not be in a situation where they are unable to terminate a service once consent is withdrawn for fear of causing an undefined "detriment" to the data subject. This provision effectively regulates the terms and conditions which organisations of services

Proposal for a regulation
Recital 34

Text proposed by the Commission	*AmCham EU Amendment*
(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	***(34) deleted***

Justification

"Significant imbalance" is too vague a standard to provide any legal certainty to data subjects or to businesses (since it could be argued that any online relationship between a service provider and a user implies a significant imbalance) and is in any case already implied in the concept of consent being freely given. Including both concepts is confusing and unnecessary.
This amendment should be combined with the deletion paragraph 4 article 7

Proposal for a regulation
Article 4, Paragraph 8 - The data subject's consent

Text proposed by the Commission	*AmCham EU Amendment*
(8) 'the data subject's consent' means any freely given specific, informed ***and explicit*** indication of his or her wishes by which the data subject***, either by a statement or by a clear affirmative action,*** signifies agreement to personal data relating to them being processed;	(8) 'the data subject's consent' means any freely given specific **and**, informed indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed;

Justification

The requirement of "explicit" consent is likely to unnecessarily disrupt the provision of services, particularly in the online environment, and is contrary to the intention specified in Recital 25 that the request must not be unnecessarily disruptive to the use of the service for which it is provided.

Proposal for a regulation
Article 7 - Conditions for consent

Text proposed by the Commission	*AmCham EU Amendment*
1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.	1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.	2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	**4. For the processing of special categories of personal data in accordance with Article 9, consent shall be explicit.**

Justification

Explicit consent is not appropriate in all circumstances, and should be reserved for situations where sensitive categories of data are concerned. Reversing the burden of proof to oblige the data controller to demonstrate consent in every context, and making the failure to do so potentially punishable by sanctions, incentivizes data controllers to authenticate users and disincentivises the provision of anonymous services or website browsing. This will increase the amount of explicitly personal data held by data controllers, the opposite of what a well-calibrated privacy regulation should achieve.

Proposal for a regulation
Article 9, Paragraph 2 - Processing of special categories of personal data

Text proposed by the Commission	*AmCham EU Amendment*
2. Paragraph 1 shall not apply where: (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8***, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or***	2. Paragraph 1 shall not apply where : (a) the data subject has given consent to the processing of those personal data, subject to the ***following*** conditions ***i. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.*** ***ii. the data subject has given his explicit consent to the processing of those data***

Justification

To be viewed in conjunction with amendments to Article 7.
It is important to reserve specific and explicit consent for the processing of sensitive data. Currently the draft Regulation makes very little distinction between sensitive data and all other data. Requiring explicit consent for the processing of every category of data makes sensitive data indistinguishable in treatment from other data, and makes it difficult for users to make choices about when it is appropriate to give or withhold their consent.

Profiling

Proposal for a regulation
Article 3, Paragraph 2 - Territorial scope

Text proposed by the Commission	*AmCham EU Amendment*
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: ***(a)*** the offering of goods or services to such data subjects in the Union***; or*** ***(b) the monitoring of their behaviour.***	2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to the offering of goods or services to such data subjects in the Union.

Justification

Read in conjunction with Recital 21, it can only be understood that this provision aims at extending the scope of the Regulation to controllers established outside the Union when their processing activities are related to the profiling of individuals. It is not justified in the text or logically why the use of a particular technique enabled by various technologies, i.e. profiling, should be used as a criterion to define the extraterritorial scope of this Regulation. Not least, since this provision does not specify uses or applications or sectors targeted but rather takes a one-size-fits-all approach towards profiling. Such a provision would clearly go against the principle of technology neutrality included in Recital 13. It is also not clear how this would be enforceable in law.

Proposal for a regulation
Article 20 - Measures based on profiling

Text proposed by the Commission	*AmCham EU Amendment*
1. ***Every natural person*** shall ***have the right*** not ***to*** be subject to a ***measure*** which ***produces legal effects concerning this natural person or significantly affects this natural person,*** and which is based solely on automated processing intended to evaluate certain personal aspects relating to this ***natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.***	1. ***A data subject*** shall not be subject to a ***decision*** which ***is unfair or discriminatory***, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this ***data subject.***
2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:	**2.** ***deleted***
(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or	
(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or	**3.** ***deleted***
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.	**4.** ***deleted***
3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.	**5.** ***deleted***
4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the	

existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. 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 suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

Justification

Para 1:

- *Article 20 essentially prohibits profiling techniques and enabling technologies across sectors and irrespective of the objectives pursued showing no recognition of the many positive uses of profiling. It demonises the technology rather than aiming to limit the existing or potential negative uses of this technology whilst protecting beneficial uses. In addition, it does not take into account the fact that there are different levels of risk associated with profiling and disparate types of impact on the privacy of individuals also related to the sensitivity of the data processed with profiling. Therefore a one-size-fits-all approach is not appropriate.*
  *Furthermore, the chosen terms **"produces legal effects"** and "**significantly affects"** are very broad, unclear and not defined in the Regulation or other EU law.*
  *Therefore the proposed amendment aims to focus the prohibition on the negative uses of profiling techniques which are either **"unfair"** or **"discriminatory"** rather than the technology itself and therefore is also in line with the technology neutrality principle of Recital 13.*
  *As defined in Directive 2005/29/EC on Unfair Commercial Practices (Article 5§2), a decision is **"unfair"** if:*
  (a) it is contrary to the requirements of professional diligence, and
  (b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product (or service) of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.
  The Guidance on the Unfair Commercial Practices Directive issued by the European Commission and the national enforcers, offers further clarification on terms such as "professional diligence, "to materially distrort" and "average consumer".

- *The term **"measure"** targets the use of profiling technologies and techniques, rather than how those may be applied to a single individual which is actually the concern here. It is suggested to revert to the language of the existing Directive and therefore replace this word with "decision".*

- *Following the suggested amendment to this, the list of examples included at the end no longer applies.*

Para 2, 3, 4, 5: *Following the proposed amendments to paragraph 1 introducing a blank prohibition of unfair or discriminatory profiling without exceptions paragraphs 2, 3, 4 and 5 should be deleted.*

Proposal for a regulation
Recital 58

Text proposed by the Commission	*AmCham EU Amendment*
(58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.	**(58)** ***Unfair or discriminatory profiling shall be prohibited. As defined in Article 5§2 in Directive 2005/29/EC on Unfair Commercial Practices, the decision referred to in Article 20 of this Regulation is "unfair" if:*** ***(a) it is contrary to the requirements of professional diligence, and*** ***(b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product (or service) of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.*** ***The Guidance on the Unfair Commercial Practices Directive issued by the European Commission and the national enforcers, offers further clarifications to this definition.***

Justification

In line with proposed amendment on Article 20.

Proposal for a regulation

Text proposed by the Commission	*AmCham EU Amendment*
References to profiling or Article 20 in Recitals 51, 59, 129 and Articles 15 paragraph 1(h), 43 paragraph 2(e), 79 paragraph 6(d).	**Deletion** of references to profiling or Article 20 in Recitals 51, 59, 129 and Articles 15 paragraph 1(h), 43 paragraph 2(e), 79 paragraph 6(d).

Justification

For consistency with proposed amendment on deletion of Article 20.

Proposal for a regulation
Recital 74

Text proposed by the Commission	*AmCham EU Amendment*
Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards~~.~~	***deleted***
[…]	***[…]***

Justification

In line with changes to Article 34.

2. Definition of personal data / Processing for security and anti-abuse purposes

Proposal for a regulation
Article 4, Paragraphs 1, 2 and *2a, 2b (new)*

Text proposed by the Commission	*AmCham EU Amendment*
(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means ***reasonably likely to be used by*** the controller ***or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;***	(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means ***available in the effective control of*** the data controller ***and as part of a specific processing operation in its regular course of business in a way that permits the controller to confirm the identity of the data subject with any appropriate means;***
(2) 'personal data' means any information relating to a data subject;	(2) 'personal data' means information relating to a data subject ***that makes identification by the controller reasonably possible;***
	(2a) 'pseudonymous data' means any personal data that has been collected, altered or otherwise processed so that it of itself cannot be attributed to a data subject without the use of additional data which is subject to separate and distinct technical and organisational controls to ensure such non attribution;
	(2b) 'anonymous data' means information that does not relate to a data subject or has been collected, altered or otherwise processed so that it cannot be attributed to a data subject;

Justification

Recitals 23 and 24 recognize that context can be a factor in determining whether data identifies a data subject, and that data which does not identify a data subject is not personal data. These important insights should be reflected in the definitions.

Proposal for a regulation
Recital 39

Text proposed by the Commission	*AmCham EU Amendment*
(39) ***The processing of*** personal 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 unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.	(39) ***It is lawful to process*** personal data to the extent strictly necessary for the purposes of ***(i) preserving network resilience and service quality; (ii)*** 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; (iii) of preventing and monitoring fraud.*** This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Justification

Self explanatory.

Proposal for a regulation
Article 6 - Amendments on the lawfulness of processing

Text proposed by the Commission	*AmCham EU Amendment*
1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(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;
(d) processing is necessary in order to protect the vital interests of the data subject;	(d) processing is necessary in order to protect the vital interests of the data subject;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(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 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;***
	(fa) processing is necessary by the controller or a third party for the purposes of preserving network resilience and service quality, of ensuring 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 or confidentiality of stored or transmitted data and the security of the related services offered by or accessible via these networks and systems, or of preventing and monitoring fraud.
2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.	2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.
3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:	3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:
(a) Union law, or	(a) Union law, or
(b) the law of the Member State to which the controller is subject.	(b) the law of the Member State to which the controller is subject.
The law of the Member State must meet an objective ofpublic interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.	The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.
4. Where the purpose of further processing is not	4. Where the purpose of further processing is not

compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.	compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.	***5. deleted***

Justification

The computer security industry needs to process data such as IP addresses to stop online attacks and protect EU citizens and organisations like banks, hospitals and schools from cyber threats such as denials of services, botnets, hacking, spam and phishing. Security processors' inability to process data classed as personal, even in contexts where they cannot attribute it to any specific individual, may result in the online security, safety and privacy of EU citizens being compromised.

Proposal for a regulation
Article 10

Text proposed by the Commission	*AmCham EU Amendment*
If the data processed by a controller ***do not permit the controller to identify a natural person,*** the controller shall ***not*** be obliged to acquire additional ***information*** in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	***1.*** If the data processed by a controller ***or a processor acting on its behalf is only pseudonymous, neither*** the controller ***nor any processor acting on its behalf*** shall be obliged to acquire additional ***information, nor to develop the means to engage in any additional processing of personal data*** for the sole purpose of complying with any provision of this Regulation. ***2. (new) In such cases, the processing shall not be subject to Articles 15 to 19, and to Article 32.*** ***3. (new) The processing of personal data for the purpose of rendering the data anonymous or to remove the controller's ability to infer the identity of a natural person from the data processed shall not be subject to Articles 15 to 19, and to Article 32.***

Justification

Ensuring the data is secure during the process of anonymisation (since at this stage it remains personal data) is necessary. But since this type of processing will aim to ensure the data can no longer be related to any identified or identifiable person, any further requirements under this Regulation would only pose unnecessary burdens to competent authorities and businesses without effectively advancing the protection of privacy.

Likewise, a data controller may also process data that does not allow identification, and it should be made clear that if a data controller is not able to identify a natural person from the information processed, then processing can be done lawfully, without either having to gain more information in order to identify an individual, or being subject to further unnecessary obligations such as seeking consent.

Proposal for a regulation
Article 14, Paragraph 1(a) new

Text proposed by the Commission	*AmCham EU Amendment*
	1(a). Where the processing of personal data is subject to Article 10, the controller may provide the information referred to in Article 14(1) via an online or offline contact point only.

Justification

Consistency with the amendment proposed to article 10.

Proposal for a regulation
Article 14, Paragraph 5 (ca) new

Text proposed by the Commission	*AmCham EU Amendment*
	(ca) (new) the data are not collected from the data subject and processing takes place on the basis of Article 6(1)(fa); or

Justification

Consistency with the proposed addition of article 6(1)(fa) In situations in networking and information security processing where it is possible to identify the data subject (for example, an ISP which has a direct relationship with their subscribers and can map IP addresses to individuals), it is preferable to undertake certain processing without informing the data subject at the time, such as when there is a compromised machine sending spam and other circumstances where one is using the data to track the control traffic and identify the real malicious actors further up the chain.

Proposal for a regulation
Recital 50

Text proposed by the Commission	*AmCham EU Amendment*
However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the	However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, ***where it would***

provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

prejudice network and information security or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

Justification

Consistency with the proposed addition of article 14(5)(ca).

Proposal for a regulation
Article 15 paragraph 2(a) new

Text proposed by the Commission | *AmCham EU Amendment*

2a. Paragraphs 1 and 2 shall not apply where processing takes place for the purpose defined in Article 6(1)(fa) and the application of paragraphs 1 and 2 would be incompatible with that purpose.

Justification

Consistency with the proposed addition of article 6(1)(fa). The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services.

Proposal for a regulation
Recital 51

Text proposed by the Commission | *AmCham EU Amendment*

Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which

Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which

recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. ***However, the result of these considerations should not be that all information is refused to the data subject.***	recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect ***network and information security or*** the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.

Justification

Consistency with the proposed addition of article 15 (2a).

Proposal for a regulation
Article 17, Paragraph 3 (da) new

Commission proposal	**Proposed amendment**
	(da) for the purpose of processing as defined in article 6(1)(fa);

Justification

Consistency with the proposed addition of article 6(1)(fa).

Proposal for a regulation
Article 30, Paragraph 3 (new)

Text proposed by the Commission	*AmCham EU 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 lawful processing pursuant to Article 6 paragraph 1 (fa).

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 lawful processing in line with the proposed Article 6(1) (fa) *new*. 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.

3. The Right to Erasure / Portability of Data

Proposal for a regulation
Recital new

Text proposed by the Commission	*AmCham EU Amendment*
	(new) Individuals that determine the purposes and the means of the processing of personal data falling outside the private household exception are also data controllers of such data; this is without prejudice to the fact that in some instances online platforms can act on behalf of the individuals and in others, these online platforms can be considered controllers, when they determine the purposes of the processing and do not act under the instructions of the individual.

Justification

In the current networked society it is important to acknowledge that data subjects too can be controllers of personal data they post and share through online platforms. These platforms are intermediaries when they act on behalf of the data subject, but can also be controllers of the personal data only if they too determine the purposes of the processing that are not determined by the data subject.

Proposal for a regulation
Recital 53

Text proposed by the Commission	*AmCham EU Amendment*
(53) Any person should have the right to have personal data concerning them rectified and a ***'right to be forgotten'*** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. ***This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.*** However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in	(53) Any person should have the right to have personal data concerning them rectified and ***the*** right to ***have such personal data erased*** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. However***, certain exemptions should apply, particularly when identifying all relevant personal data in question proves impossible or involves a disproportionate effort and when in relation to personal data made publicly available by the data subject himself or herself, such right is overridden by the interests or fundamental rights and freedoms of others. An exemption should also apply to enable the data controller to process data for their***

the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.	***legitimate interest, as for instance for the purpose of providing system, network or information security. T***he further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

Justification

The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. However certain exemptions should apply to recognise that:

It is not always possible for a controller to identify all of the related personal data (for instance, where a third party makes information about another individual available online).

The right of erasure may be overridden by the interests or fundamental rights and freedoms of others.

An exemption should apply when a controller wishes to process the information for certain legitimate purposes such as for the purpose of providing system, network or information security.

Proposal for a regulation
Recital 54

Text proposed by the Commission	*AmCham EU Amendment*
(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.	***(54) deleted***

Justification

It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms.

Furthermore, these provisions might generate negative unintended consequences in the online environment

whereby, in order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

Proposal for a regulation
Recital 121

Text proposed by the Commission	*AmCham EU Amendment*
(121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.	(121) The processing of personal data solely ***for the purpose of exercising the right to freedom of expression, including for the purposes of journalistic, artistic or literary expression*** for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field, ~~*and*~~ in news archives, ~~*and*~~ ***in*** press libraries, ***and in the use of other means of communication, including the internet and social media***. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

Justification

The proposed amendment is aimed at clarifying the notion of freedom of expression. It is important to recognize in the Regulation the right of others to know and to publicise certain facts concerning a data subject, as this is closely linked to the right to freedom of expression and other democratic values.

Proposal for a regulation
Article 4 - Definitions

Text proposed by the Commission	*AmCham EU Amendment*
	(20) (new) 'Applicable national law': is the law of the place where the controller has its main establishment in accordance with this Regulation.

Proposal for a regulation
Article 3, Paragraph 4 (new)

Text proposed by the Commission	*AmCham EU Amendment*
	3 (4) (new) For the purposes of compliance with the obligations of this Regulation, the applicable law is to be determined in accordance with Article 4 and 51 of the Regulation.

Justification

The Regulation does not clarify what national law is applicable in cases where this Regulation builds on national legislation. The internal market cannot be fragmented in cases of personal data processing.

Proposal for a regulation
Article 17, Paragraph 1

Text proposed by the Commission	*AmCham EU Amendment*
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, ***especially in relation to personal data which are made available by the data subject while he or she was a child,*** where one of the following grounds applies:	1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data where one of the following grounds applies:
(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which	(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the

the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

Except where:

(e) identifying all relevant personal data in question proves impossible or involves a disproportionate effort;

(f) such right is overridden by the interests or fundamental rights and freedoms of others.

Justification

The right to erasure in Article 17(1) is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. The right to erasure should be reviewed to recognize that the right balance is struck between the rights of a data subject to get their data deleted, the rights of individuals to remember and the right to freedom of expression. The practical difficulties associated with identifying the necessary information to ensure compliance with this provision must also be taken into account. Certain exemptions should apply to recognise that:

- *It is not always possible for a controller to identify all of the related personal data (for instance, where a third party makes information about another individual available online);*
- *The right of erasure may be overridden by the interests or fundamental rights and freedoms of others;*
- *A controller should be able to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security*

Moreover, the right to be forgotten in Article 17(2) needs very careful consideration It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms.

Furthermore, this provision might generate negative unintended consequences in the online environment whereby, in order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

Proposal for a regulation
Article 17

Text proposed by the Commission	*AmCham EU Amendment*
2. ***Where the controller referred to in paragraph 1 has made the personal data public,*** it shall take all reasonable steps, including technical measures, in relation to data ***for the publication*** of which the controller is responsible, to inform third parties ***which are processing*** such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. ***Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.***	2. ***In cases where the Controller, other than the data subject to whom the information pertains*** has transferred the personal data to third parties, it shall take all reasonable steps, including technical measures, in relation to data **processing for** which the controller is responsible, to inform third parties **to whom such data has been transferred** that a data subject requests them to erase any links to, or copy or replication of that personal data.

Justification

In the online networked world, natural persons can determine the means and the purposes for which information related to them can be processed; for instance, a social platform can be chosen by the data subject, as well as the purposes for which the information should be processed on his behalf. However, in these situations, it cannot be excluded completely that more than one controller processes the information. Against this background, the additional duty to inform third parties needs to be framed in the context of the distinct responsibilities of each of the actors, in line with ECJ Jurisprudence.

Proposal for a regulation
Article 17, Paragraph 8

Text proposed by the Commission	*AmCham EU Amendment*
8. Where the erasure is carried out, the controller shall not otherwise process such personal data.	***8. deleted***

Justification

Complete erasure as opposed to restriction of personal data processing can have a detrimental effect on the ability of data subjects to exercise other rights, such as access and rectification requests, and the possibility of the controller to verify and proof compliance with such requests.

4. Administrative burden and data controller/ data processor issues

Proposal for a regulation
Article 4, Paragraph 5

Text proposed by the Commission	*AmCham EU Amendment*
(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, ***conditions and means*** of the processing of personal data; where the purposes***, conditions and means*** of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, of the processing of personal data; where the purposes, of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

Proposal for a regulation
Article 24 - Joint controllers

Text proposed by the Commission	*AmCham EU Amendment*
24. Where a controller determines the purposes, ***conditions and means*** of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	24. Where a controller determines the purposes***,*** of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. ***The arrangement shall duly reflect the joint controllers' respective effective roles and direct or indirect relationship with data subjects.***

Proposal for a regulation
Recital 62

Text proposed by the Commission	*AmCham EU Amendment*
(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, ***conditions and means*** of the processing jointly with other controllers or where a processing operation is carried out on	(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes***,*** of the processing jointly with other controllers or where a processing operation is carried out on behalf of a

behalf of a controller.	controller***, due account being taken of their respective roles and direct or indirect relationship with data subjects***.

Justification

Under the proposed Regulation, data "controllers" and data "processors" are subject to different obligations. In light of this framework, it is important that the Regulation include a clear test that organisations can apply to determine when they are operating as controllers and when they are operating as processors. The amendment above would introduce such a clear test.

*As a general rule, controllers typically determine **why** data is processed (i.e. for what purposes) while processors typically determine **how** it is processed (i.e. under what conditions). In a scenario where a cloud service provider offers enterprise customers a hosted email service, for example, the provider is likely to be a data processor. That's because the cloud service provider only determines "how" the data is processed -- i.e. it stores and delivers email for the purposes and at the direction of its enterprise customers. However, if the cloud service provider also uses the email addresses it collects from the service to profile end users and send them spam, then the cloud service provider has a say in the "why" the data is processed and becomes a data controller. In this scenario, the cloud service provider will be a controller for the same data for which it is a data processor.*

Unhelpfully, however, the test proposed under the Regulation confuses the simple "how" and "why" distinction -- making it harder for organisations to determine whether they are a controller or a processor or both. Under the Regulation, controllers are defined as those that determine not only the "purposes" of processing data (i.e. the "why"), but also the "conditions and means" of processing (i.e. the "how"). As the European Parliament's study has concluded, this approach isn't clear.

The above amendment would address this confusion by deleting the reference to "conditions and means," and making clear that the data controller is the entity that determines the "purposes" of the processing only -- i.e. the entity that determines the "why" data is processed. This change will help to clarify the divide between the important roles of controller and processor and create greater legal certainty.

In addition, for joint controllers, the arrangement should be expressly required to duly reflect the joint controllers' respective roles and relationship with the data subjects, to ensure that joint controllers are on a level playing field. Joint controllers are indeed not necessarily in an equal negotiation position. Moreover, joint controllers have not all equal access to data subjects nor do they control the same kind and amount of personal data.

Proposal for a regulation
Article 14, Paragraphs 1 and 5 - Information to the data subject

Text proposed by the Commission	*AmCham EU Amendment*
1.Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:
(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;	(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer ***or, if appropriate, the identity and contact details of the group of undertakings and its data protection officer***;
(b) the purposes of the processing for which the personal data are intended***, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)***;	(b) the purposes of the processing for which the personal data are intended;
(c) the period for which the personal data will be stored;	***(c) deleted***
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;	(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
(e) the right to lodge a complaint to the supervisory authority ***and the contact details of the supervisory authority***;	(e) the right to lodge a complaint to the ***lead*** supervisory authority;
(f) the recipients or categories of recipients of the personal data;	(f) ***where material,*** the recipients or categories of recipients ***outside the controller or the group of undertakings of which the controller is a member*** of the personal data;
(g) where ***applicable***, that the controller intends to transfer to a third country or international organisation ***and on the*** level of protection ***afforded by that third country or international organisation by reference to an adequacy decision by the Commission;***	(g) where ***material***, that the controller intends to transfer to a third country or international organisation ***that does not provide an adequate*** level of protection;
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.
[.....]	[.....]
5. Paragraphs 1 to 4 shall not apply, where: (a) the data subject ***has*** already the information referred to in paragraphs 1, 2 and 3; or	5. Paragraphs 1 to 4 shall not apply, where: (a) the data subject already ***has or can reasonably be expected to know*** the information referred to in

	paragraphs 1, 2 and 3; or

Proposal for a regulation
Recital 48

Text proposed by the Commission	*AmCham EU Amendment*
(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, ***how long the data will be stored***, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.	(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

Justification

There should be greater flexibility and less prescription regarding the information to be provided to the individual, as a part of fair processing notice. The current draft is too prescriptive and would create huge administrative and cost burdens for organizations, without delivering a real benefit for individuals. In global organizations, with global processes and global systems, it is impossible to customise notices for each data controller in the group of undertakings, especially where the information in the notices is same, save for the name of data controller and/ or DP Officer. Furthermore, long and complex notices are never read by individuals, they are cumbersome to draft and deliver effectively and just create work for lawyers – detracting from their main purpose, which is to provide information to individuals that they care about , did not know or can do something about. The long prescriptive list should be made more flexible by including the words "where material" – allowing for flexibility to provide certain information only where that is of essence or important for individual.

It is often difficult, if not impossible, to state accurately how long personal data will be stored as it can depend on unknown factors such as legal proceedings arising. As a result, a requirement to state how long personal data are stored will in many cases lead to generic statements such as "for as long as necessary for the purposes for which the personal data are processed" which does not provide a data subject with any greater transparency or clarity. The requirement to specify the third country destination of a data transfer in the information to the data subject would be unnecessarily burdensome, and should be limited to instances where the third country/organization do not offer an adequate level of protection.

Proposal for a regulation
Article 15, Paragraph 2(a) new - Right of access for the data subject

Text proposed by the Commission	*AmCham EU Amendment*
	2(a) (new) Paragraphs 1 and 2 shall not apply where processing takes place for the purpose defined in Article 6(1)(fa) and the application of paragraphs 1 and 2 would be incompatible with that purpose.

Justification

Consistency with the proposed addition of article 6(1)(fa). The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services.

Proposal for a regulation
Article 22 - Responsibility of the controller

Text proposed by the Commission	*AmCham EU Amendment*
1.The controller shall ***adopt policies and*** implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller, ***or the group of undertakings of which the controller is a member,*** shall implement appropriate measures to ensure and be able to demonstrate ***upon request*** that the processing of personal data is performed in compliance with this Regulation.
2. The measures provided for in paragraph 1 shall in particular include:	2. The measures provided for in paragraph 1 shall in particular include:
keeping the documentation pursuant to Article 28;	
(a) implementing the data security requirements laid down in Article 30;	***a) management commitment and oversight to ensure processing of personal data is carried out in compliance with this Regulation, including, if appropriate, the appointment of the Data Protection Officer pursuant to Article 35.1;***
(b) performing a data protection impact assessment pursuant to Article 33;	***b) policies and procedures that document the requirements of this Regulation including the security requirements laid down in Article 30;***
(c) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	***c) an assessment of risks associated with the processing of personal data such as, but not limited to, data protection impact assessments as required under Article 33;***
(d) designating a data protection officer pursuant to Article 35(1).	
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by	

independent internal or external auditors.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying ***any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards*** the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

d) appropriate documentation of processing activities as laid out in Article 28

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

Justification

Most global companies have global data privacy compliance programmes and these are set at global and group company level rather than for each controller. Moreover, the list of measures should be more flexible, listing what constitutes effective compliance without going into prescriptive detail on each of them. The measures should be aligned to the globally emerging accountability model , the Binding Corporate Rules requirements and especially the Corporate Data Management Framework, published by the Canadian Privacy Commissioners. Finally, the measures which the controller must undertake are clearly outlined in paragraph 2. As such, there is no need for the Commission to give itself powers to determine further requirements or criteria, or indeed to define the structure for audits.

Proposal for a regulation
Article 26 - Processor

Text proposed by the Commission

1. Where ***a*** processing ***operation*** is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

AmCham EU Amendment

1. Where processing is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller ***as to the purposes of the processing***, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) ***hand over all results to the controller after the end of the processing and*** not process the personal data ***otherwise***;

(h) make available to the controller ***and the supervisory authority*** all information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall ***be subject to the rules on joint controllers laid down in Article 24***.

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 responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) ***where the processor*** enlist***s*** another processor ***solely to perform specific processing operations for the controller, enlist such other processor*** only with the prior permission of the controller;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) not process the personal data further ***after the end of the agreed processing except where the personal data are anonymised, retained for compliance purposes or for the purposes referred to in point (g) of paragraph 1 of Article 6***;

(h) ***upon request*** make available to the controller all ***relevant and permissible*** information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall ***comply with all applicable provisions of this Regulation.***

5. deleted

Justification

The proposed text introduces a host of new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice. There are situations where processor uses another processor to perform certain processing operations or provide services to the processor organization, that are not related and specific to any particular controller. For example,

processor should be able to decide on business continuity and recovery services, hosting services, cloud services, or any other IT services which many third party processors provide to a processor organization, without having to ask permission of controller whose data are in the mix and may be included in these services. Controller should have a right to approve sub-processors only where they may be directly performing sub- processing services related to the contract between the controller and processor. In relation to handing over results at the end of processing, there may be no results as such to hand over if the data minimisation principle has been effectively applied, e.g. where the data is anonymised, or where such data should be retained for compliance purposes. There are also instances where a processor is required to process controller's personal data for their own purposes, for example in order to ensure information security in respect of controller's data, or to ensure business continuity. Such processing should be allowed and not subject to any contractual restrictions. Making data available to the supervisory authority should be handled by the controller. Certain information may be subject to a confidentiality obligation under law or contract and hence a processor may not be at liberty to disclose such information to a supervisory authority. Moreover, such data should not be required to be transmitted on a regular basis as this would overburden authorities and further increase the administrative burden. Equally, in the instances where processor uses controller's personal data for their own purposes, the processor becomes a controller, rather than joint controller. Joint controllership would put much onus on both parties and would imply they share the same purposes and means of processing, which may not be true at all in the circumstances. Finally, the word "operation" should be deleted in paragraph 1 after the word "processing" in order to avoid confusion as the word "operation" is used in the definition of "processing" in Article 4(1).

In relation to the delegated act clause, the Lisbon Treaty makes clear that such acts are meant to be used to "supplement or amend certain non-essential elements" of a law. In the context of the proposed Regulation, however, the Commission often appears to be using delegated acts to determine the scope and applicability of core aspects of the law -- including with regard to fundamental issues such as the obligations of processors (Article 26(5)). The obligations of processors should be clearly defined in the Regulation itself. Europe's processors -- and the controllers and data subjects they serve -- should not be required to wait for secondary legislation to be adopted in order to understand the responsibilities, duties and tasks that apply to processors. For this reason, Article 26(5) should be deleted.

Proposal for a regulation
Article 28 - Documentation

Text proposed by the Commission	*AmCham EU 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, if any, the controller's representative, shall maintain documentation of ***the different categories of*** processing under its responsibility.
2. The documentation shall contain at least the following information:	***2. Such documentation shall include a general description of the categories of data subjects, personal data processed and purposes for which the personal data are generally processed.***
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the ***lead*** supervisory authority.
(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);	***4. Where a controller engages a processor, the controller shall be responsible for maintaining the***
(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;

(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;

(g) a general indication of the time limits for erasure of the different categories of data;

(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.

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

(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.

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).

documentation referred to in Article 28.1 and can request the processor to provide assistance in compiling the information.

5. The controller and, if any, the controller's representative, shall make the documentation available, on request, to the **lead** supervisory authority.

6. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers:

(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.

5. Deleted

7. 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).

Proposal for a regulation
Recital 65

Text proposed by the Commission	*AmCham EU Amendment*
(65) In order to demonstrate compliance with this Regulation, the controller ***or processor*** should document ***each*** processing ***operation***. Each controller ***and processor*** should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	(65) In order to demonstrate compliance with this Regulation, the controller should document ***the different categories of*** processing. Each controller should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

Justification

Requiring both controllers and processors to maintain the same documentation for the same categories of processing is an unnecessary burden that does not enhance the protection of data subjects or facilitate enforcement by the authorities. The controller should be primarily responsible for maintaining the documentation in order to avoid duplication with the processor. If the processor is given an independent duty to maintain documentation, it should be different from the controller. The level of information that controllers should be required to record should be set at much more general level. To prescribe very granular and specific items to record for each processing activity, tool, system or process would create an excessive administrative burden, something which the removal of notification duties in all Member States was designed to avoid. Transparency for individuals will be provided through timely fair processing notices, so there is no obvious benefit for the individual of the sort of detailed internal register proposed here. In groups of undertakings each member of the group is often a controller in respect of at least some personal data, e.g. HR data, but in order to use the data efficiently they will all use the same tools and processes. To require each controller to maintain documentation in relation to the same processing activity would represent a duplication and a disproportionate administrative burden. Finally, whilst the controller should carry the primary responsibility for the documentation, it is recognised that processors can provide useful information to the controller to assist them in this task.

Proposal for a regulation
Article 30 - Security of processing

Text proposed by the Commission	*AmCham EU Amendment*
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in	2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss

particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

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.

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;

(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).

and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. deleted

4. deleted

Proposal for a regulation
Recital 66

Text proposed by the Commission	*AmCham EU 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.

Justification

The security requirements under the current Directive are being effectively applied and while the new proposals make a more direct appeal to the responsibilities of processors, there is no need for the Commission to adopt additional powers in this area. This is particularly true because such security requirements should be technology neutral so as to avoid market distortion and the detailing of blueprints for malicious actors to follow. This is not compatible with the wording in the Commission's additional powers, which talks about specific technologies and solutions.

Proposal for a regulation
Article 33

Text proposed by the Commission	*AmCham EU 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 present specific risks referred to in paragraph 1:
(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for	***(a) deleted***

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;	[…]
[…]	***(e) deleted***
(e) other processing operations for which the consultation of gthe supervisory authority is required pursuant to point (b) of Article 34(2).	[…]
[…]	***4. deleted***
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.	[…]
[…]	***6. deleted***
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.	[…]
[…]	

Justification

With the view to ensure legal certainty and enable better enforcement by supervisory authorities and in accordance with Recital 62 which requires "a clear attribution of the responsibilities under this Regulation", privacy impact assessments should be carried out by the controller. Notably, the controller is in the best position to assess the impact of any processing. The controller, and not the processor, has ready access to all relevant information, including risks and benefits of processing the personal data. The PIA process should only be imposed where the "specific risks" referred to in the proposed Article (a far too imprecise and over-inclusive category) may lead to legal effects that gravely and adversely affect the individual's fundamental rights. Furthermore, the requirement to seek the views of data subjects is impractical.

Proposal for a regulation
Article 34 - Prior authorisation

Text proposed by the Commission	*AmCham EU 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 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. ***If the supervisory authority has not made a decision to grant or refuse the authorisation within three months from the date on which the request for authorisation was submitted to the supervisory authority, and one month in case a controller uses contractual clauses as provided for in point (d) of Article 42(2), the authorisation shall be deemed to be granted.***
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. deleted***
(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 present a high degree of specific risks; or	***(a) deleted***
(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) deleted***
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	***4. deleted***
	5. deleted
	6. deleted
	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

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.

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 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.

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).

ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. deleted

9. The Commission may set out standard forms and procedures for prior authorisations referred to in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Requiring prior consultation in the case of the wide range of processing operations likely to be captured within the definition of a 'high degree of specific risks' is likely to be a serious impediment to innovation in Europe, and to overwhelm the supervisory authorities. Given the prohibition that already exists in Article 20 of profiling that

causes a significant adverse effect on a data subject, prior authorisations should be reserved for processing involving sensitive categories of data. Allowing supervisory authorities to establish an ex ante list of generic categories of data processing which it considers risky would create exactly the same risk of over-broad use of the authorisation mechanism. There must also be a time limit for the supervisory authority to deliberate and communicate a decision to authorise or not. Otherwise, controllers are subject to undue delay and inefficiencies due to inability to implement systems and tools globally or across Europe at the same time.
Our understanding is that this provision focuses on transfers and have consequently deleted the words 'in particular'. We have maintained the references to processors in an attempt to allow them use contractual clauses for data transfers they handle on behalf of the controller.

Proposal for a regulation
Recital 74

Text proposed by the Commission	*AmCham EU Amendment*
(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.	***(74) deleted***

Justification

Requiring prior consultation in the case of the wide range of processing operations that may qualify for a 'high degree of specific risks', in accordance with the long list in Article 33, is likely to be a serious impediment to innovation in Europe. DPAs could face a deluge of cases that quickly back-up and may in numerous instances have to refer those cases to the European Data Protection Board in accordance with proposed Article 58.2 (a), without there being any imposed reasonable time-limit (i.e. no longer than three months) on the supervisory authorities/European Data Protection Board to adopt any measure further to such consultation, thereby potentially bringing to a halt and crippling innovation and activities. Even if the DPAs and the European Data Protection Board had the resources to handle the case-load (quod certe non), conducting a thorough investigation is likely to be a case of months, not days. An ex-post system is far more fitting to a regime of effective and accountable data protection which does not impede growth and innovation.

Proposal for a regulation
Article 35 - Designation of the data protection officer

Text proposed by the Commission	*AmCham EU Amendment*
1. The controller and the processor ***shall*** designate a data protection officer in any case where:	1. The controller and the processor ***may*** designate a data protection officer
(a) the processing is carried out by a public authority or body; or	***(a) deleted***
(b) the processing is carried out by an enterprise employing 250 persons or more; or	***(b) deleted***
(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	***(c) deleted***
	2. (new) Where the controller or processor designates a data protection officer in accordance with Article 35, 36 and 37, they will be exempt from Articles 28, 33 and 34. It will also be considered as a mitigating factor in assessing the application of administrative sanctions, in accordance with Article 79(2).
2. ***In the case referred to in point (b) of paragraph 1***, a group of undertakings may appoint a single data protection officer.	2. ***Where the (joint) controller(s) or processor(s) are part of an enterprise,*** a group of undertakings may appoint a single data protection officer.
3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.	3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	***4. deleted***
5. The controller or processor ***shall*** designate ***the*** data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	5. ***Where t***he controller or processor ~~***shall***~~ designate***s*** ~~***the***~~ ***a*** data protection officer***, they shall do so*** on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.
6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in
7. ***The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be***	

reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. 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 core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

a conflict of interests.

7. deleted

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer***, if any,*** to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer***, if any,*** on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. deleted

Proposal for a regulation
Article 36 - Position of the data protection officer

Text proposed by the Commission	*AmCham EU Amendment*
1. ***The*** controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. ***Where the*** controller or the processor ***designates a data protection officer they*** shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.
2. ***The*** controller or processor ***shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer*** shall directly report to the management of the controller or the processor.	2. ***Where the*** controller or processor ***designates a data protection officer they*** shall directly report to the management of the controller or the processor.
3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.	3. The controller or the processor shall support the data protection officer***, if any,*** in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Proposal for a regulation
Article 37 - Tasks of the data protection officer

Text proposed by the Commission	*AmCham EU Amendment*
1. ***The*** controller or the processor shall ***entrust*** the data protection officer ***at least with the following tasks:***	1. ***Where the*** controller or the processor ***designates a data protection officer they*** shall ***determine the tasks to be performed by*** the data protection officer ***in order to ensure compliance with this Regulation.***
(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;	
(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;	
(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	
(d) to ensure that the documentation referred to in Article 28 is maintained;	
(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;	
(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;	
(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;	
(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.	
2. 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 tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

Proposal for a regulation
Recital 75

Text proposed by the Commission	*AmCham EU Amendment*
(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor ***to*** monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks ***independently***.	***(75) The*** controller or processor ***may appoint a person to assist them in*** monitor***ing*** internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks ***effectively***. ***Controllers and processors should be given an incentive to appoint such data protection officers through simplification of certain compliance obligations under this Regulation.***

Justification

Under the current Directive, the text provides for incentives for data controllers to act responsibly by providing for an exemption from the general notification regime where the controller appoints a data protection official. The Regulation should reflect this ethos by reducing the administrative burden on controllers and processors who choose to adopt a responsible approach. The controller or processor in question would still have clear obligations to establish effective policies and implement appropriate measures to demonstrate compliance with the Regulation, implement privacy by design and default, undertake effectual data security, provide transparent information to the data subjects and ensure they can apply their right. However, they would have a greater degree of flexibility and ex-ante box-ticking exercises which create a significant administrative burden without significantly increasing data protection would be reduced.

Just like with any other internal compliance roles, most organizations appoint a person in charge of data privacy compliance as a permanent role, and not subject to change or re-appointment every 2 years. It is difficult to imagine that the organization would not have a right to dismiss a data protection official for poor performance, or any other misconduct during the performance of their job. Any role, including the most senior and executive roles are subject to performance review and normal business review processes – there should be no difference for the data protection official. Regarding the independence requirement, the Data Privacy Officer is able to perform their role more effectively if they are an integral part of the business. We are concerned that the proposal to ensure complete separation of the role from the business would have the adverse effect of distancing the DPO from the business and lead to less rather than greater oversight. From a practical perspective, this may preclude many current DPOs from either company share ownership or performing this role. Finally, the tasks of the DPO should not be specified to the degree envisaged in the Commission's proposal, but should rather be set by the organization in a such way to ensure compliance and oversight over compliance with the Regulation. It is a matter of each organization to determine what these tasks should be and what that means for their own operations, given particular business circumstances. It is expected that they would be in line with Art. 22 – the accountability model.

Proposal for a regulation
Article 77 - Right to compensation and liability

Text proposed by the Commission	*AmCham EU Amendment*
1. Any person who has suffered damage as a result of ***an*** unlawful processing ***operation*** or of an action incompatible with this Regulation shall have the right to receive compensation from the controller ***or the processor*** for the damage suffered.	1. Any person who has suffered damage as a result of unlawful processing or of an action incompatible with this Regulation shall have the right to receive compensation from the controller for the damage suffered.
2. Where more than one controller ***or processor*** is involved in the processing, each controller ***or processor*** shall be jointly and severally liable for the entire amount of the damage.	2. Where more than one controller is involved in the processing, each controller shall be jointly and severally liable for the entire amount of the damage***, to the extent that the joint controllers' respective liability has not already been established in the determination of responsibilities envisaged in Article 24.***
	3. If a processor processes personal data for purposes other than as instructed by the controller, both parties may be held liable should any person suffer damage as a result of such processing.
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

Justification

Under the current Directive, liability is correctly attributed to the data controller. Essentially, they direct the data processor and if the processor does not act on those orders then contractual arrangements apply to address the circumstances. Introducing a vague liability clause does not clarify the current situation but creates confusion for controllers, processors and data subjects alike. The joint and several liability referred to in paragraph 2 should only apply to joint controllers where they have not determined their respective responsibilities and liabilities in a legal arrangement, as required in article 24.

Proposal for a regulation
Article 91 - **Application of the Regulation**

Text proposed by the Commission	*AmCham EU Amendment*
1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.	1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from [*two years from the date referred to in paragraph 1*].	2. It shall apply from [two years from the date referred to in paragraph 1] ***to new processing of personal data created on or after the date referred to in paragraph 1. Articles [24, 26, 28, 33, 34(1), 34(2)…] shall apply three years thereafter to processing of personal data existing prior to the date referred to in paragraph 1***.

Justification

The bringing into compliance of processing of personal data existing prior to the Regulation will be extremely resource- and time-consuming, especially for industries where existing processing involve literally tens of thousands of partners, thereby requiring tens of thousands of agreements to be revisited. The exact list of Articles to which the five year derogation applies depends on the final form of the adopted provisions.

5. Fines / Remedies

Proposal for a regulation
Article 79 - **Administrative Sanctions**

Text proposed by the Commission	*AmCham EU Amendment*
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.	1. ***Without prejudice to other sanctions and remedies, the lead*** supervisory authority shall ***have the authority to*** sanction the administrative offences listed in paragraphs 2 to 6.
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach and the degree of co-operation with the supervisory authority in order to remedy the breach.	2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, ***the sensitivity of data in question,*** the intentional or negligent character of the infringement, ***the degree of harm or risk of significant harm created by the violation,*** the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23, ***whether the natural or legal person has appointed a data protection officer in accordance with Article 35*** and the degree of co-operation with the supervisory authority in order to remedy the breach. ***In setting an administrative fine, supervisory authorities shall also take into account fines, damages or other penalties previously imposed by a court or other body on the natural or legal person regarding the same violation.***
4. The supervisory authority ***shall*** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: […]	***2(a) Aggravating factors that support administrative fines at the upper limits established in paragraphs 2-6 shall include in particular:***
5. The supervisory authority ***shall*** impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: […]	***(i) repeated violations committed in reckless disregard of applicable law,***
6. The supervisory authority ***shall*** impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, ***intentionally or negligently:*** […]	***(ii) refusal to co-operate with or obstruction of an enforcement process, and***
j) does not designate a data protection officer or does not ensure the conditions for fulfilling the	***(iii) violations that are deliberate, serious and likely to cause substantial damage.***

tasks pursuant to Articles 35, 36 and 37;	***2(b) Mitigating factors which support lower or no administrative fines at all shall include***
	(i) measures taken by the natural or legal person to ensure compliance with relevant obligations,
	(ii) genuine uncertainty as to whether the activity constituted a violation of the relevant obligations,
	(iii) immediate termination of the violation upon knowledge, and
	(iv) Co-operation with any enforcement processes.
	4. The ***lead*** supervisory authority ***may*** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover ***up to a maximum of 500 000 EUR*****,** to anyone who, ***in deliberate violation of the law or with reckless disregard for applicable obligations***:
	5. The ***lead*** supervisory authority ***may*** impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover ***up to a maximum of 1 000 000 EUR***, to anyone who, ***in deliberate violation of the law or with reckless disregard for applicable obligations***:
	[…]
	6. The ***lead*** supervisory authority ***may, at its discretion,*** impose a fine up to 1 000 000 EUR, or in case of an enterprise up to 2 % of its annual worldwide turnover ***up to a maximum of 2 000 000 EUR***, to anyone who, ***in deliberate violation of law or with reckless disregard for applicable obligations***:
	[…]
	[Deletion]

Justification

These amendments modify the proposal in four areas:

- *First, the amendments specify the mitigating and aggravating factors that supervisory authorities should consider when imposing fines. In doing so, the amendments ensure that higher fines are imposed on more serious misconduct, and also encourage compliance and cooperation once a violation is discovered. Specifying these factors will also promote greater consistency across the Member States in terms of the fines imposed.*

- *Second, the amendments proposes to replace the term "shall" by "may" as it relates to Supervisory Authorities. This is to avoid burdensome and bureaucratic procedures for minor infringements and to emphasize that there are circumstances under which such administrative fines would be disproportionate. It is up to the independence and discretion of the Supervisory Authority to decide how to use this sanction.*

- *Third, the amendments make it clear that where an individual or an entity has already been subject to a sanction in another proceeding for the same violation (such as a civil judgment), that fact should be considered in assessing a fine. This avoids penalizing a party twice for the same conduct.*

- *Finally, the amendments reflect the fact that while deliberate or reckless violations of the proposed Regulation should merit substantial penalties, imposing the same penalties on merely negligent violations would be disproportionate. The proposed amendments allow supervisory authorities to impose administrative fines that constitute meaningful deterrents; at the same time, these provisions ensure that the most punitive sanctions are reserved for truly bad actors.*

If the Commission nonetheless concludes that negligent conduct should also be covered in the Regulation, it's crucial to specify the language on how negligence should be assessed:

1. The supervisory authority may also impose administrative sanctions in the case of negligent violations of the provisions identified in paragraphs 4, 5 and 6. In cases of negligent violation, the administrative fine shall be set at the lower limit of the ranges established in paragraphs 4, 5 and 6, and shall take into account the criteria referred to in paragraphs 2, 2(a) and 2(b).

2. Negligent violations are those where the natural or legal person:

(i) fails to take appropriate measures to ensure that the processing of personal data is performed in compliance with its obligations;

(ii) does not commit the violation deliberately or with reckless disregard of the relevant obligations; and

(iii) in committing the violation, exposes the data subject(s) to substantial risk of harm.

The deletion in paragraph 6 relating to the data protection officer is in line with our proposed changes to Article 35, which create incentives for organisations to appoint data protection officers through a reduction in the administrative burden, as opposed to a mandatory approach. This would free resources to improve data protection throughout the organisation as opposed to focusing on mere compliance.

6. Applicable Law (One-Stop-Shop / "Main Establishment/Lead DPA/Consistency) / Governance Principles and Transparency

Proposal for a regulation
Recital 135

Text proposed by the Commission	*AmCham EU Amendment*
(135) This Regulation ***should*** apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive ***should*** be amended accordingly.	(135) This Regulation ***shall*** apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive ***shall*** be amended ***by this Regulation*** accordingly.

Justification

The word 'shall' clarifies that necessary amendments to Directive 2002/58/EC to avoid inconsistencies in the law are to be undertaken by this Regulation and not at a later stage.

Proposal for a regulation
Article 3, Paragraph 2

Text proposed by the Commission	*AmCham EU Amendment*
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:	2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are ***specifically targeted at such data subjects in order*** to:
(a) the offering of goods or services to such data subjects in the Union; or	(a) ***offer*** goods or services to ***them***; or
(b) the monitoring of their behaviour.	(b) ***monitor*** their behaviour.

Justification

The simple availability of a foreign e-commerce website to be accessed and viewed by individuals in the EU should not in itself fall under the "offering of goods and services to EU residents". Likewise, general web

analytics, used by the operators of websites around the globe that may be visited by individuals from the EU, should not by themselves fall under the monitoring of EU residents' behaviour. For this provision to be more relevant to the effective protection of EU data subjects' rights, it should cover those controllers whose offers or monitoring activities specifically target data subjects residing in the EU, e.g. a Korean company offering websites in multiple European languages.

One-Stop-Shop / "Main Establishment"/Lead DPA/Consistency

Proposal for a regulation
Recital 27

Text proposed by the Commission	*AmCham EU Amendment*
(27) The main establishment ***of a controller in the Union*** should be determined according to objective ***criteria and should imply the effective and real exercise of*** management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. ***The main establishment of the processor should be the place of its central administration in the Union.***	(27) The main establishment ***in the Union of an undertaking or of a group of undertakings, whether a controller, a processor or both,*** should be determined according to objective ***criteria, i.e. the location of the undertaking's or group's European headquarters, or the location where*** management activities ***are effectively exercised,*** determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.

Justification

Today, enterprises operating across the Union find themselves required to comply with multiple and often diverging national data protection regimes. This situation creates legal uncertainty and impedes the free flow of data in the Union.

The proposed Regulation seeks to improve this situation by subjecting enterprises that are processing data in the Union to a single law and a single supervisory authority in the country of "main establishment" (the so-called "one-stop-shop"). This is a significant step forward. Greater harmonisation will dramatically reduce the compliance burdens on European organisations while at the same time ensuring a high level of protection for data subjects.

Less helpful, however, in determining the location of an organisation's "main establishment," the Regulation applies a different test for controllers and processors. This approach ignores the fact that some controllers are

also processors. In these cases, it makes little sense to apply different tests. Doing so will result in these controllers once again faced with the need to comply with multiple regimes.

The amendment above takes a more sensible approach, and applies the same test to controllers and processors in those cases where the controller is also acting as a processor. This approach ensures that such controllers are fully able to benefit from the one-stop-shop that is the centrepiece of the proposed Regulation.

Proposal for a regulation
Recital 28

Text proposed by the Commission	*AmCham EU Amendment*
(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. ***A group of undertakings may nominate a single main establishment in the Union.***

Justification

The amendment clarifies that a group of undertakings can be viewed as a single entity responsible to a single supervisory authority. The simplification achieved by nominating a single point of contact should not be undermined by various supervisory authorities viewing individual controlled undertakings as separate data controllers or processors.

Proposal for a regulation
Recital 63

Text proposed by the Commission	*AmCham EU Amendment*
(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a	(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the ***provision*** of goods or services to such data subjects, the controller should designate a representative, unless the controller

representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally providing goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory ***authority in accordance with Article 51 of this Regulation.***

Justification

There is no justification to deny the application of the internal market approach to companies that are not established in the EU, but that name a representative in the territory of the Union. As the Regulation provisions apply, article 51 should also apply. Related to ''provision'' is clearer than ''offering''.

Proposal for a regulation
Recital 65

Text proposed by the Commission

(65) In order to demonstrate compliance with this Regulation, the controller or ***processor*** should document ***each*** processing ***operation.*** Each controller ***and processor*** should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

AmCham EU Amendment

(65) In order to demonstrate compliance with this Regulation, the controller or ***its representative in the Union, where applicable,*** should document ***the different categories of*** processing ***of personal data***. Each controller should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations

Justification

Requiring both controllers and processors to maintain the same documentation for the same categories of processing is an unnecessary burden that does not enhance the protection of data subjects or facilitate enforcement by the authorities. The controller should be primarily responsible for maintaining the documentation in order to avoid duplication with the processor. If the processor is given an independent duty to maintain documentation, it should be different from the controller. The level of information that controllers should be required to record should be set at much more general level. To prescribe very granular and specific items to record for each processing activity, tool, system or process would create an excessive administrative burden, something which the removal of notification duties in all Member States was designed to avoid. Transparency for individuals will be provided through timely fair processing notices, so there is no obvious benefit for the individual of the sort of detailed internal register proposed here. In groups of undertakings each member of the group is often a controller in respect of at least some personal data, e.g. HR data, but in order to use the data efficiently they will all use the same tools and processes. To require each controller to maintain

documentation in relation to the same processing activity would represent a duplication and a disproportionate administrative burden. Moreover, whilst the controller should carry the primary responsibility for the documentation, it is recognised that processors can provide useful information to the controller to assist them in this task. Finally, it is important that the Regulation recognises the different responsibilities and tasks of controllers and the representative, in case of non EU based companies to whom the Regulation applies.

Proposal for a regulation
Recital 97

Text proposed by the Commission	*AmCham EU Amendment*
(97) Where the processing of personal data ***in the context of the activities of an establishment of a controller or a processor in the Union*** takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.	(97) Where the processing of personal data takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.

Justification

The draft Regulation should be clear that the one-stop shop principle applies consistently for both EU and non-EU based controllers subject to the law.

Proposal for a regulation
Recital 105

Text proposed by the Commission	*AmCham EU Amendment*
(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, ***or to the*** monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also	(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, ***including*** monitoring such data subjects, ***where the non-EU controller or processor has not appointed a representative in***

apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

the EU, or that might substantially affect the free flow of personal data. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

Justification

There is no justification to exclude the representative from the internal market rules applicable to other legal or natural persons established in the EU for the purposes of the application of this Regulation.

Proposal for a regulation
Article 4, Paragraph 13

Text proposed by the Commission	*AmCham EU Amendment*
(13) 'main establishment' means as regards ***the*** controller, ***the place of its establishment in the Union where*** the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data ***are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;***	(13) 'main establishment' ***in the Union*** means as regards ***an undertaking or a group of undertakings, whether*** controller***, processor or both, the European headquarters of the undertaking or group of undertakings, or the location where effective and real management activities are exercised and/or*** main decisions ***are taken*** as to the purposes, conditions and means of the processing of personal data.

Proposal for a regulation
Article 4, Paragraph 14

Text proposed by the Commission	*AmCham EU Amendment*
(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;	(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller ***or the processor,*** acts instead of the ***controller or the processor,*** with regard to the obligations of the controller ***or the processor*** under this Regulation;

Justification

There is no justification to exclude the representative from the internal market rules applicable to other legal or natural persons established in the EU for the purposes of the application of this Regulation.

Proposal for a regulation
Article 4 paragraph 19 (a) (new)

Text proposed by the Commission	*AmCham EU Amendment*
	19(a) (new) 'lead supervisory authority' means the supervisory authority of the main establishment of the controller or processor in accordance with article 51 paragraph 2.

Justification

This new definition is meant to bring clarity as to the effective implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 12, Paragraph 3

Text proposed by the Commission	*AmCham EU Amendment*
3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the ***lead*** supervisory authority and seeking a judicial remedy.

Justification

This amendment is meant to effectively implement the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 15, Paragraph 1 (f)

(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	(f) the right to lodge a complaint to the ***lead*** supervisory authority and the contact details of the ***lead*** supervisory authority;

Justification

This amendment is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 29

Text proposed by the Commission	*AmCham EU Amendment*
1. The controller and the processor and, if any, the	1. The controller and the processor and, if any, the

representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	representative of the controller, shall co-operate, on request, with the ***lead*** supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.
2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	2. In response to the ***lead*** supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 31, Paragraph 1

Text proposed by the Commission	*AmCham EU Amendment*
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 lead to significant risk of substantial harm to a data subject***, the controller shall without undue delay after having ***confirmed that a personal breach has occurred***, notify the personal data breach to ***its lead*** supervisory authority.

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 32, Paragraphs 3 and 4

Text proposed by the Commission	*AmCham EU Amendment*
3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that 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.	3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the ***lead*** supervisory authority that it has implemented appropriate technological protection measures, and that 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.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the ***lead*** supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 39, Paragraph 9

Text proposed by the Commission	*AmCham EU Amendment*
9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	9. The controller or the processor shall communicate the name and contact details of the data protection officer to the ***lead*** supervisory authority and to the public.

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 43, Paragraphs 2 (j) and (k)

Text proposed by the Commission	*AmCham EU Amendment*
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;	(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the ***lead*** supervisory authority;
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	(k) the co-operation mechanism with the ***lead*** supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the ***lead*** supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 43, Paragraphs 3

Text proposed by the Commission	*AmCham EU 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 requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	***3. Where a processor wishes to provide appropriate safeguards by binding corporate rules as referred to in point (a) of paragraph 2 of Article 42, the matters referred to in points (a) to (k) of paragraph 2:*** ***(a) shall only apply to the extent they are applicable to the processor and are material to the data subject and*** ***(b) can be specified in relation to each controller.***

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 44, Paragraph 6

Text proposed by the Commission	*AmCham EU Amendment*
6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.	6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the ***lead*** supervisory authority of the transfer.

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 52, Paragraph 1 (b)

Text proposed by the Commission	*AmCham EU Amendment*
(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article **73, investigate,** to the extent ***appropriate***, the **matter** and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further **investigation or** coordination with another supervisory authority is necessary;	(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article **73;**, to the extent ***that it has competence in accordance with article 51 paragraph 2, investigate*** the ***matter; or, if it does not have competence, refer the matter in accordance with the provisions of Section 1 of Chapter VII to the lead supervisory authority;*** and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further ***investigation,*** coordination with ***or referral to*** another supervisory authority is necessary;

Justification

This provision is essential to conciliate the right of data subjects or of their representatives and associations to lodge complaints with the authority of their choice on the one hand, and the concept of one lead authority for each controller or processor on the other hand.

Proposal for a regulation
Article 53

Text proposed by the Commission	*AmCham EU Amendment*
(paragraph 1)	(paragraph 1 unchanged)
	1(a) (new) Powers referred to in points (a) to (h) of paragraph 1 are conferred upon the lead supervisory authority in accordance with article 51 paragraph 2. A supervisory authority that is not the lead supervisory authority in the meaning of article 51 paragraph 2 may in accordance with Section 1 of Chapter VII request the lead supervisory authority to exercise such powers in relation to a controller or processor under that supervisory authority's competence:
2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:	2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor ***under its competence in accordance with article 51 paragraph 2***:

Justification

This provision is essential to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 58, Paragraphs 2, 3 and 4

Text proposed by the Commission	*AmCham EU Amendment*
2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:	2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:
(a) relates to 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	(a) relates to processing activities **of personal data including the monitoring of behaviour** which are related to the offering of goods or services to data subjects in several Member ***States when the non-EU controller or processor does not name a representative in the territory of the European Union;*** or
(b) may substantially affect the free movement of personal data within the ***Union; or***	(b) may substantially affect the free movement of personal data within the ***Union.***
(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or	***(c) deleted***
(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or	(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or
(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or	(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or
(f) aims to approve binding corporate rules within the meaning of Article 43.	***(f) Deleted***
3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, ***in particular*** where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.	3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.
4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.	***4. deleted***

Justification

There is no justification to discriminate against non- EU companies that are covered by the Regulation, by automatically applying the consistency mechanism to these companies. Where the non EU company names a representative in the EU, there is no need to submit these companies to the data protection board in all circumstances. The competence of the data protection board to non- EU companies that are entirely covered by

the Regulation should be equivalent to EU companies. If the non EU company does not name a representative, it is justified. Please see also comments on point 3. The list of processing operations subject to prior consultation should be determined in the regulation and not left to DPAs, because that in itself leads to inconsistency (each DPA naming different lists). The consistency mechanism needs to be an exceptional mechanism and not a body of appeal of legitimate decisions of the lead DPA. Otherwise the consistency mechanism becomes an appeal mechanism that slows decision taking and becomes a bureaucratic step in detriment of all actors.

Proposal for a regulation
Article 86, Paragraph 2

Text proposed by the Commission	*AmCham EU Amendment*
2. The delegation of power referred to in ***Article 8(3), Article 9(3),*** Article 12(5), Article 14(7), Article 15(3), ***Article 17(9), Article 20(5), Article 22(4),*** Article 23(3), ***Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(7),***[1] Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	2. The delegation of power referred to in Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

Proposal for a regulation
Article 86, Paragraph 3

Text proposed by the Commission	*AmCham EU Amendment*
3. The delegation of power referred to in ***Article 8(3), Article 9(3),*** Article 12(5), Article 14(7), Article 15(3), ***Article 17(9), Article 20(6), Article 22(4),*** Article 23(3), ***Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(7),*** Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

[1] *Note that this Article is mis-cited in the proposed Regulation as Article 79(6). The correct reference is to Article 79(7).*

Proposal for a regulation
Article 86, Paragraph 4

Text proposed by the Commission	*AmCham EU Amendment*
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. ***The Commission shall present proposals for delegated acts to be adopted pursuant to Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) within two years of the date of publication of this Regulation in the Official Journal of the European Union.*** As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

Proposal for a regulation
Article 86, Paragraph 5

Text proposed by the Commission	*AmCham EU Amendment*
5. A delegated act adopted pursuant to ***Article 8(3), Article 9(3),*** Article 12(5), Article 14(7), Article 15(3), ***Article 17(9), Article 20(6)***, ***Article 22(4),*** Article 23(3), ***Article 26(5), Article 28(5), Article 30(3)***, ***Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(7),*** Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.	5. A delegated act adopted pursuant to Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Justification

Of the 91 articles in the Regulation, 26 include provisions that would allow the Commission to adopt "delegated acts." Each delegated act provision empowers the Commission to create new, secondary legal regimes, binding across the EU.

The many delegated act provisions mean that organisations could face new rules for many years after the Regulation is adopted. This creates confusion about data subjects' rights. It also makes it difficult for organisations processing data to understand their obligations. Because the Regulation includes substantial sanctions for non-compliance (up to 2% of annual worldwide turnover for certain violations), it is critical that organisations understand clearly what their obligations are.

To address these issues, the number of delegated acts should be significantly reduced. Delegated acts should be used only where needed and appropriate. Specifically:

1. ***Consistent with the Lisbon Treaty, any delegated act provisions that deal with essential elements of the law should be deleted.*** *Many of the delegated act provisions -- including Article 9(3), Article 22(4), Article 26(5), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 43(3), Article 44(7) and Article 79(7) -- address essential elements of the data protection framework. However, under the Lisbon Treaty, delegated acts are intended to supplement "non-essential elements" of the Law. Essential issues should be addressed in the Regulation, not deferred until a later date. Allowing the Commission to defer legislating on essential elements of the law undermines legal certainty and makes it difficult for companies to plan for compliance. These Articles should be deleted.*

2. ***Consistent with EU policy, those delegated acts that allow the Commission to dictate how technologies should be developed should also be deleted.*** *Certain delegated acts provisions -- including Article 8(3), Article 17(9) and Article 30(3) -- threaten to undermine the principle of technology neutrality by allowing the Commission to adopt prescriptive rules, standards and formats. Technology neutrality is well established in European law and policy. Technology neutral policies allow for competition among different solutions, which in turn drives innovation. At the same time, technology neutrality ensures that legislation is not "frozen in time," as technology evolves. But by allowing the Commission to dictate how obligations should be implemented at a technical level, these provisions give the Commission the power to substitute regulatory intervention for industry innovation. Again, these Articles should be deleted.*

3. ***Delegated acts that remain in the Regulation should be subject to a clear timetable for adoption.*** *Without a clear timeline for the adoption of delegated acts, controllers, processors and data subjects could face a lengthy period of uncertainty about their obligations and their rights. The Article 29 Working Party has acknowledged this concern, stating in its Opinion on the proposal that "At the very least the Working Party calls on the Commission to set out which delegated acts it intends to adopt in the short, medium and long term."*

[Corresponding amendments will need to be made to Recital 129 and Recital 131 and Article 6(5), Article 8(3), Article 9(3), Article 17(9), Article 20(5), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), and Article 79(7).]

Governance Principles and Transparency

Proposal for a regulation
Recital 61

Text proposed by the Commission	*AmCham EU Amendment*
(61) ***The*** protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures ***are*** taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. ***In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.***	(61) ***To meet consumer and business expectations around the*** protection of the rights and freedoms of data subjects with regard to the processing of personal data, appropriate organisational measures ***may be*** taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. ***Measures having as an objective to increase consumer information and ease of choice shall be encouraged, based on industry cooperation and favouring innovative solutions, products and services.***

Proposal for a regulation
Recital 110 (a) *(new)*

Text proposed by the Commission	*AmCham EU Amendment*
	(110) (a) The European Data Protection Board should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, data subjects' associations, consumer organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Board on a proposal by the Chair, should focus on issues relevant to all stakeholders and bring them to the attention of the Board. The Chair may, where appropriate and according to the agenda of the meetings, invite representatives of the European Parliament and other relevant bodies to take part in meetings of the Group.

Justification

Consistency with the new Article 70(a) proposed below.

Proposal for a regulation
Recital 129

Text proposed by the Commission	*AmCham EU Amendment*
(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal ***data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of […] criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default;***	(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, ***appropriate industry lead measures and policies shall take due account of the principles of technology, service and business model neutrality so as to favour the free movement of personal data within the Union.***

Proposal for a regulation
Recital 130

Text proposed by the Commission	*AmCham EU Amendment*
(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No	***(130) In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.***

182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

Proposal for a regulation
Article 23

Text proposed by the Commission	*AmCham EU Amendment*
1. Having regard to the state of the art and the cost of implementation, ***the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet*** the requirements of this Regulation and ensure the protection of the rights of the data subject.	1. Having regard to the state of the art***,*** the cost of implementation ***and international best practices***, ***appropriate measures and procedures may be put in place to ensure the processing operation meets*** the requirements of this Regulation and ensure***s*** the protection of the rights of the data subject.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	***2. Such measures and procedures shall:*** • ***take due account of existing technical standards and regulations in the area of public safety and security*** • ***follow the principle of technology, service and business model neutrality*** • ***be based on global industry-led efforts and standards*** • ***take due account of international developments***
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.	***3. In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.***
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***4. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and***

communications, and consistent with international industry-led standardisation efforts.

Justification

Privacy by Design/Default (PbD) is a concept currently being discussed internationally, relating to internal privacy and data protection processes for organizations based on a number of factors including their business models, size and interaction with personal data. Although every organisation should strive to integrate privacy and data protection into its internal processes, the actual way it does so should remain flexible and leave room for adaptation based on their business models, size and interaction with personal data. This is to say that there is no one right way which is especially true in the case of SMEs, given their specific circumstances and for entities that are far removed from processing identifiable personal data. It is essential that any PbD concept be technology-neutral and not introduce specific technology or operational mandates, or contribute to a differentiation between ICT and other economic sectors. The concept should therefore focus on designing privacy into processes and people and should maintain as a key objective providing consumers with appropriate tools to make an informed choice. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies to flourish in the spirit of the European Digital Agenda. There is also a clear need to look into the issue with a global perspective to avoid further fragmentation, taking stock of industry's own efforts and taking technology developments into account.

Proposal for a regulation
Article 70 paragraph 1 point (aa) *(new)* - Permanent Stakeholders' group

Text proposed by the Commission	*AmCham EU Amendment*
	(aa) convene the meetings of the Permanent Stakeholders' Group and prepare its agenda;

Justification

Consistency with the new Article 70a proposed below.

Proposal for a regulation
Article 70(a) *(new)* - Permanent Stakeholders' Group

Text proposed by the Commission	*AmCham EU Amendment*
	1. The European Data Protection Board shall set up a Permanent Stakeholders' Group on a proposal by the Chair, composed of experts representing the relevant stakeholders, such as but not limited to relevant private sector players, data subjects' associations, consumer groups and academic experts in privacy and data protection.
	2. Procedures for, in particular, the number, composition, and appointment of the members by the Board, proposal by the Chair and the operation of the Group shall be specified in the Board's internal rules of operation and shall be made public.
	3. The Group shall be chaired by the Chair of the Board.
	4. The term of office of the Group's members shall be two-and-a-half years. Members of the Board may not be members of the Group. Commission staff shall be entitled to be present at the meetings and participate in the work of the Group.
	5. The Group shall advise the Board in the performance of its activities and tasks.

Justification

Like data controllers and processors, the EDPB should also be accountable and transparent in guiding the interpretation and enforcement of the regulatory framework. The consultation and decision making mechanism proposed here is meant to ensure that the Board and supervisory authorities pursue an ongoing transparent dialogue with all interested stakeholders, including the private sector, data subjects, and academia, for the shared benefit of all involved parties.

Proposal for a regulation
Article 71, Paragraph 3

Text proposed by the Commission	*AmCham EU Amendment*
3. The secretariat shall be responsible in particular for:	3. The secretariat shall be responsible in particular for:
(a) the day-to-day business of the European Data Protection Board;	(a) the day-to-day business of the European Data Protection Board;

(b) the communication between the members of the European Data Protection Board, ***its chair*** and the Commission and for communication with other institutions and the public;	(b) the communication between the members of the European Data Protection Board, ***the members of the Permanent Stakeholder Group, the Chair*** and the Commission and for communication with other institutions and the public;
(c) the use of electronic means for the internal and external communication;	(c) the use of electronic means for the internal and external communication;
(d) the translation of relevant information;	(d) the translation of relevant information;
(e) the preparation and follow-up of the meetings of the European Data Protection ***Board;***	(e) the preparation and follow-up of the meetings of the European Data Protection ***Board and of the Permanent Stakeholders' Group;***
(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection ***Board.***	(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection ***Board, as well as of documents of the Permanent Stakeholders' Group.***

Justification

Consistency with the new Article 70(a) proposed above.

Proposal for a regulation
Article 72 - Confidentiality and publicity

Text proposed by the Commission	*AmCham EU Amendment*
1. The discussions of the European Data Protection Board shall be ***confidential.***	1. The discussions of the European Data Protection Board shall ***only*** be ***confidential in so far as and to the extent that they relate to specific cases. Discussions pursuant to the carrying out of the tasks of general interest laid down in points (a), (b), (c), (e),(f) and (g) of paragraph 1 of Article 66, as well as, to the extent that they do not relate to specific cases, the discussions pursuant to the adoption of opinions under the consistency mechanism in accordance with Article 58 shall be public.***
2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.	2. Documents ***relating to specific cases*** submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.
3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the	3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the

confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon ***them.***	confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon ***them where applicable. The chair shall also ensure the appropriate publicity of discussions not falling under a confidentiality requirement.***

Justification

The EDPB has a major advisory and interpretation role with respect to the general privacy regime and its implementation. Data subjects, data controllers, data processors, representatives of the European and national legislators, as well as supervisory authorities themselves and all other relevant stakeholders should have the opportunity to be informed of the discussions of general interest and general relevance that will be pursued in the EDPB.

7. Certification / Codes of Conduct

Proposal for a regulation
Article 38

Text proposed by the Commission	*AmCham EU Amendment*
1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the ***proper application of*** this Regulation***, taking account of the specific features of the various data processing sectors, in particular in relation to:*** ***(a) fair and transparent data processing;*** ***(b) the collection of data;*** ***(c) the information of the public and of data subjects;*** ***(d) requests of data subjects in exercise of their rights;*** ***(e) information and protection of children;*** ***(f) transfer of data to third countries or international organisations;*** ***(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;*** ***(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75***.	1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the ***protection of personal data or to compliance with*** this Regulation. ***Particular encouragement shall be given to European-level codes of conduct.***
2. Associations and other bodies representing categories of controllers or processors in one Member State ***which intend to draw up*** codes of conduct or ***to*** amend or extend ***existing*** codes of conduct ***may submit them*** to an opinion of the supervisory authority in that Member State. The supervisory authority may give ***an*** opinion whether the draft code of conduct or the amendment is ***in compliance*** with this Regulation. The supervisory authority shall seek the views of ***data subjects or their representatives*** on these ***drafts***.	2. Associations and other bodies representing categories of controllers or processors in one Member State ***may submit new*** codes of conduct or amend***ments*** or exten***sions to*** existing codes of conduct to an opinion of the supervisory authority in that Member State ***on a voluntary basis***. The supervisory authority may give ***a non-binding*** opinion ***on*** whether the draft code of conduct or the amendment ***or the extension contributes to the protection of personal data or to compliance*** with this Regulation. The supervisory authority may seek the views of ***all stakeholders*** on these ***codes, in which case it shall deliver its opinion within 90 days***.
3. Associations and other bodies representing categories of controllers in several Member States may submit ***draft*** codes of conduct and amendments or extensions to existing codes of conduct to the	3. Associations and other bodies representing categories of controllers in several Member States may submit ***new*** codes of conduct and amendments or extensions to existing codes of conduct to the

Commission.	Commission. ***These initiatives should be fully in line with existing legal obligations and not aim at preventing the free circulation of goods and services in the internal market.***
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	4. The Commission may adopt ***non-binding opinions on whether*** the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 ***contribute to the protection of personal data, or are compatible with this Regulation, or contribute to compliance with it. In addition, the Commission's opinions shall consider whether the codes of conduct contribute to the functioning of the Internal Market. The Commission shall seek the views of all stakeholders on these codes, and shall deliver its opinion within 90 days***. ***4(a) (new) The opinions of the supervisory authorities and of the Commission pursuant to paragraphs 2 and 4 shall be a separate matter from formal determinations of individual operators' compliance with the law.***
5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.	5. The Commission shall ensure appropriate publicity for the codes which have been ***the subject of positive opinions*** *in accordance with paragraph* ***4(a) (new)***.
Proposal for a regulation **Article 39 - Certification**	
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.	1. The Member States and the Commission shall ***work with controllers, processors and other stakeholders to*** encourage ***voluntary*** data protection certification mechanisms and data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. ***Such*** mechanisms shall, in cases where clear legal obligations do not exist: • ***be voluntary, affordable, and available via a process that is transparent and not unduly burdensome*** • ***take due account of existing security measures and regulations in the area of public safety and security*** • ***follow the principle of technology, service and business model neutrality*** • ***be elaborated in consultation with the Member States Data Protection Authorities*** • ***be based on industry lead efforts and standards*** • ***take due account of international developments***
2. 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 data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.	
3. The Commission may lay down technical standards	

for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

2. (Based on Article 14 of the ePrivacy Directive) - In implementing the provisions of this Regulation, Member States shall ensure, that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications and consistent with international industry lead standardisation efforts.

4. ***National data protection authorities [N.B. or the EU board, if it is going to be created] shall be the repositories of such data protection certification mechanisms and data protection seals and marks, thus providing for easy access for citizen.***

Justification

Industry- developed and managed certification should be favoured, provided they remain voluntary and affordable. Such certifications should be open to companies both inside and outside the EEA in order to facilitate international data flows and be elaborated in consultation with the relevant stakeholders. They should enable competition and be industry driven and favor innovative solutions for the consumers. Indeed, industry is able to adapt to new market realities at a faster pace than government, and government does not have the same competitive incentive to enforce proper use of certifications (e.g. icons or seals on web pages) as industry does. In the long term, an industry-developed and managed certification that is endorsed by both EU and non-EU regulators would help reduce compliance burdens on operators and foster competitiveness. Certification mechanisms shall however not be used to create discrimination between sectors or value chains. Specifically, certification schemes would need to:

- ***Be based on industry lead standards and practices.***
- *Be **developed with stakeholder input at EU level**. To help create effective schemes and encourage widespread adoption, Member States and the Commission should work with stakeholders to establish the process of developing EU level certifications, seals and marks.*
- *Be **voluntary**. Mandatory certification schemes can chill innovation and deter competition in the development of enhanced privacy protections.*
- *Be **affordable**. Some privacy certification regimes involve costs of upwards of €150,000 simply to certify one feature of a product or service. These costs create barriers to entry for all but the largest service providers, and discourage wide-scale use of the regime.*
- *Be available via a process that is **transparent and not unduly burdensome**. To ensure organisations apply for and adopt certifications, seals and marks that give individuals confidence about how their data is being processed, the process to apply for and be awarded a mark should not be unduly bureaucratic or burdensome.*

- *Be capable of being **rolled-out and recognised globally**. To help reduce the compliance burden on providers, any certification scheme should be capable of being endorsed by regulators in third countries as well as by those in the Union.*
- *Be **neutral** as to system, service, platform or technology. Similarly situated services and products should be subject to the same assessment criteria. Favouring some solutions over others creates market distortions and hinders innovation.*

Proposal for a regulation
Article 42, Paragraph 1

Text proposed by the Commission	*AmCham EU Amendment*
1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.	1. Where the Commission has taken no decision pursuant to Article 41, ***or has not taken a positive decision pursant to Articel 41(3)*** a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

Proposal for a regulation
Article 42, Paragraph 2 (b) and (c)

Text proposed by the Commission	*AmCham EU Amendment*
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: …	2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: …
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or	(b) standard data protection clauses ***between the controller or processor and the recipient of the data outside the EEA, which may include standard terms for onward transfers outside the EEA***, adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or
(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or …	(c) standard data protection clauses ***between the controller or processor and the recipient of the data outside the EEA, which may include standard terms for onward transfers outside the EEA***, adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or …

Justification

In its Study on "Reforming the Data Protection Package", the Parliament's Policy Department points out that under the proposed Regulation, standard clauses do not extend to agreements between processors and sub-processors. As the Study points out, this gap could significantly disadvantage European firms, including new technology start-ups. The Article 29 Working Party has also recognised the need for sub-processors to be subject to the same obligations as apply to processors with regard to transferred data.

The amendment above is designed to close this gap. Data processors often subcontract processing activities to other companies, and such arrangements are now routine in the context of cloud computing. But without standard clauses -- a key tool enabling international data transfers -- European enterprises will be placed at a competitive disadvantage as they will be restricted from choosing sub-processors outside of Europe.

For example, a European cloud start-up (the data processor) may build the service it offers to customers on technology offered by a third party (the sub-processor). Without standard clauses to protect the flow of data to sub-processors outside of the Union, the cloud start-up will be restricted in its choosing platforms on which to build its service -- and may, as a result, ultimately be forced to offer a cloud service that is less competitive.

In line with the Study's recommendation, the amendment above explicitly allows the Commission and Member States to extend standard clauses to sub-processors. This will give EU-based cloud providers and others greater flexibility and freedom in choosing adequate sub-processors.

Proposal for a regulation
Article 42 – paragraph 2 (e) (new)

Text proposed by the Commission	*AmCham EU Amendment*
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: …	2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: … ***(e) contractual clauses between the controller or processor and the recipient of the data that supplement standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and are authorised by the lead supervisory authority in accordance with paragraph 4.***

Proposal for a regulation
Article 42, Paragraph 3

Text proposed by the Commission	*AmCham EU Amendment*
3. A transfer based on standard data protection clauses or binding corporate rules asreferred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.	***3. The appropriate safeguards referred to in paragraph 1 may also be provided by a single legally binding instrument between the processor and another processor that impose substantively the same obligations on the sub processor as the EU standard data protection clauses adopted by the***

Commission where a processor is engaged by multiple controllers to carry out substantively similar processing operations in relation to their respective personal data and such personal data of multiple controllers are transferred to another processor in a third country:
a) by the processor and/or
b) by the controller

Proposal for a regulation
Article 42, Paragraph 4

Text proposed by the Commission	*AmCham EU Amendment*
4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.	4. Where a transfer is based on contractual clauses as referred to in point (d) ***or (e)*** of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the ***lead*** supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the ***lead*** supervisory authority shall apply the consistency mechanism referred to in Article 57.

Justification
This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

Proposal for a regulation
Article 42, Paragraph 5

Text proposed by the Commission	*AmCham EU Amendment*
5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.	5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the ***lead*** supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the ***lead*** supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

Proposal for a regulation
Article 44, Paragraph 1

Text proposed by the Commission	*AmCham EU Amendment*
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: […]	1. In the absence of an adequacy decision pursuant to Article 41***; or where the Commission decides that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5);*** or ***in the absence*** of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: […]

Justification

The wording of the Draft could rule out all forms of data transfers to the country, territory, sector or international organization considered as not offering an adequate level of protection regardless of whether other appropriate safeguards are put in place. Article 41(6) of the Draft indeed provides that the prohibition to

transfer personal data in case of inadequacy decided by the Commission is "without prejudice to Articles 42 to 44" while Articles 42(1) and 44(1) mention that they apply only if the Commission has not taken any decision on adequacy.

Proposal for a regulation
Article 44, Paragraph 1 (h)

Text proposed by the Commission	*AmCham EU Amendment*
h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.	h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive ***or where, prior to such transfer, the personal data is already made lawfully public in the third country***, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

Justification

What this proposal acknowledges is that a data controller exporting public domain information back into a third country where is it already publicly available must remain responsible for adducing appropriate safeguards. However it also acknowledges that as the information is already widely known in that third country, the export poses a different level of risk for the data subject when compared to an export of consumer provided data. As the result of such reduced risk, it is not appropriate to impose the full requirements of Article 42 but instead the proposal provides the data controller with a degree of discretion around how it discharges its legal responsibilities.

Proposal for a regulation
Recital 84

Text proposed by the Commission	*AmCham EU Amendment*
(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. ***In some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust***

safeguards via additional contractual commitments that supplement standard data protection clauses.

Proposal for a regulation
Recital 85

Text proposed by the Commission	*AmCham EU Amendment*
(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.	(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, ***as well as to processors acting under its instructions,*** as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

Justification

Realities of data processing today require the recognition of the variety of actors participating in the data processing. This is needed not to water down the provisions of this regulation but to reinforce them. Therefore the legal recognition of different actors can only increase the levels of efficiency and enforceability of data protection by extending these to agents acting on behalf of controllers and processors that are engaged in different phases of the processing of personal data. Finally, the provision on biding corporate rules (article 43) indicates that binding corporate rules are binding not only internally (ie within the group of undertakings, but also externally, and that the controller or processor signing the BCR remains liable; therefore it is not justified to exclude agents on behalf of the controller or processor.

Proposal for a regulation
Article 42, Paragraph 4

Text proposed by the Commission	*AmCham EU Amendment*
4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.	4. Where a transfer is based on contractual clauses as referred to in point (d) ***or (e)*** of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the ***lead*** supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the ***lead*** supervisory authority shall apply the consistency mechanism referred to in Article 57***.***

Proposal for a regulation
Article 42, Paragraph 4 (a) (new)

Text proposed by the Commission	*AmCham EU Amendment*
	4(a) (new) To encourage the use of supplemental contractual clauses as referred to in point (e) of paragraph 2 of this Article, lead authorities may offer a data protection seal, mark or mechanism, adopted pursuant to Article 39, to controllers and processors who adopt these safeguards.

Justification

This amendment encourages data controllers and processors to apply the strongest protections possible to data they transfer outside of the Union.

With the increasing globalisation of business and the evolution of computing models like the cloud, cross-border flows of personal data have become routine. In this environment, it is critical that controllers and processors apply strong safeguards to personal data regardless of where that data is located. Users will only have confidence in cloud computing if they know that their data is safe in the cloud.

The current Directive (95/46) generally prohibits transfers of data outside of the Union, however, unless the receiving country has been deemed by the Commission to offer "an adequate level" of data protection. Where a country has not been deemed "adequate", a company can only transfer data if it can rely on an exception in the Directive, such as using "standard contractual clauses" that the Commission or national DPAs have approved.

Standard clauses are widely used today by organisations that transfer data. Effectively, they impose a legally binding obligation on organisations outside of the Union to apply certain "baseline" protections to data that has been transferred from the Union, including requirements to implement adequate security measures to protect data. The clauses also regulate liability for any damages suffered by individuals between the companies that export and import the data, and enable individuals whose data has been transferred to enforce certain provisions.

In many cases, it may be appropriate for organisations to apply additional safeguards to protect data being transferred out of Europe -- i.e. to supplement the standard clauses with even more robust protections. The amendment above makes clear that organisations can do this, and also creates an incentive to adopt these supplemental protections in the form of a data protection seal or trust mark, which would foster innovation in privacy.

Specifically, the amendment proposed above would do two things:

(1) make clear that controllers and processors may supplement standard contractual clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation with additional contractual commitments, thereby offering stronger protections to customers; and

(2) encourage controllers and processors to adopt these heightened commitments by offering them a data protection "seal of approval". The seal or trust mark could be adopted pursuant to Article 39 of the Regulation.

Proposal for a regulation
Article 42, Paragraph 5(a) (new)

Text proposed by the Commission	*AmCham EU Amendment*
	5(a) (new) In the event of a discrepancy between the Regulation and the legal requirements of the requesting third country, the Commission will strive to resolve the conflicting legal situation during which the data controller or processor cannot be held liable.

Justification

Private organisations should not be put in the middle of conflicting legal requirements within the European Union or between the EU and third countries.

9. Definition of a Child

Proposal for a regulation
Article 6 (f)

Text proposed by the Commission	*AmCham EU 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 or freedoms of the data subject which require protection of personal data, ***in particular where the data subject is a child.***	(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 or freedoms of the data subject which require protection of personal data.

Proposal for a regulation
Recital 38

Text proposed by the Commission	*AmCham EU Amendment*
(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. ***This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection.*** The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.

Proposal for a regulation
Article 33, Paragraph 2 (d)

Text proposed by the Commission	*AmCham EU Amendment*
2 (d) The following processing operations in particular present specific risks referred to in paragraph 1: (…) (d) personal data in large scale filing systems on ***children***,	2 (d) The following processing operations in particular present specific risks referred to in paragraph 1: (…) (d) personal data in large scale filing systems on genetic data, or biometric data.

genetic data, or biometric data.

Proposal for a regulation
Recital 29

Text proposed by the Commission	*AmCham EU Amendment*
(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. ***To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child. This Regulation should define a child as an individual under the age of 13.***	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data***. For the purpose of this Regulation a child should be defined*** as an individual under the age 13.

Proposal for a regulation
Article 4, Paragraph 4 (18)

Text proposed by the Commission	*AmCham EU Amendment*
4 (18) 'child' means any person below the age of ***18*** years;	4 (18) 'child' means any person below the age of ***13*** years;

Justification

A threshold of 13 years of age for a child reflects more accurately the prevailing standard in Europe (though there are some variations). This prevailing standard has already been reflected in the Regulation's Article 8, which specifies that the processing of the data of a child under 13 shall be lawful only with parental consent. This general threshold should be consistent with the consent threshold already established in the Regulation.

10. Data Breach

Proposal for a regulation
Recital 67 - Security Breach Notification

Text proposed by the Commission	*AmCham EU Amendment*
(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller ***becomes aware*** that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay ***and, where feasible, within 24 hours***. ***Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification.*** The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.	(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller ***has confirmed with a reasonable degree of certainty*** that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay. ***This means that notification is not immediately required after an incident has occurred but only once the controller has been able to determine with a reasonable degree of certainty that the incident is a personal breach.*** The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

Justification

The requirement to notify within 24 hours is unrealistic and may prejudice investigations and cause unnecessary distress to consumers. The priority should be to investigate a breach and take appropriate action to limit any loss or damage to consumers.

Proposal for a regulation
Recital 68 - Confirmation of security measures taken following security breach

Text proposed by the Commission	*AmCham EU Amendment*
(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.	(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. ***In order to avoid over-notification to individuals and supervisory authorities and to ensure efficient use of resources, only those breaches identified as having negative and harmful consequences should be notified.***

Justification

Not all breaches threaten user privacy. For example, the loss of a file contacting the names and addressed of data subjects that are in the public domain, would not lead to harm for the consumers concerned as the data are publicly available. Reporting the loss to consumers and supervisory authorities is unwarranted in such cases. In order for the EU's regime to be workable, the notification must focus on personal data breaches that are likely to have serious and negative consequences rather than all breaches.

Proposal for a regulation
Article 31, Paragraph 1

Text proposed by the Commission	*AmCham EU Amendment*
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 lead to significant risk of substantial harm to a data subject***, the controller shall without undue delay notify the personal data breach to ***its lead*** supervisory authority.

Proposal for a regulation
Article 31 (a) (new)

Text proposed by the Commission	*AmCham EU Amendment*
	31 (a) (new) ***Notification of a personal data breach shall not be required if the controller demonstrates to the satisfaction of the lead authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible or unusable to any person who is not authorised to access it.***

Proposal for a regulation
Article 31, Paragraph 5

Text proposed by the Commission	*AmCham EU Amendment*
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. deleted***

Proposal for a regulation
Article 32, Paragraph 1

Text proposed by the Commission	*AmCham EU Amendment*
1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. ***Upon determination by the lead supervisory authority,*** when the personal data breach is likely to ***lead to significant risk of substantial harm to*** the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

Justification

Breach notice obligations provide important incentives to data controllers to be responsible in their management of data, and will help to drive a higher standard of data security across industry. Requiring notice of breaches also fosters confidence of data subjects in third party processing.

To be effective, the breach notice regime must be practical and workable. The regime should not overly burden DPAs nor should it require that controllers notify breaches that prove harmless, which could lead data subjects to suffer from "notification fatigue". To achieve these ends, the amendments above make three important changes to the proposed Regulation:

- ***First, the amendments would eliminate the obligation to notify within 24 hours.*** *There is significant consensus among industry and regulators that notice within 24 hours is not feasible. Controllers need more time to understand the nature of the breach, who is affected, and whether the breach poses harm to the data subjects involved.*
- ***Second, the amendments make clear that notice is required only where the breach threatens significant risk of serious harm to the data subject.*** *Notifying harmless breaches could have unintended effects: to begin with, it is likely to cause unwarranted anxiety among data subjects, but ultimately may lead to data subjects ignoring all notices. A requirement to notify harmless breaches would also burden data controllers and DPAs unnecessarily, leading to increased costs for European businesses. In addition, lacking resources to deal with these notifications, DPAs may miss important data breaches. In order to ensure a healthy and trustworthy environment, data breaches should be treated appropriately based on the likelihood of harm resulting from the breach.*
- ***Third the usability of the data and the circumstances in which the data was lost should also be considered in determining whether notification is needed.*** *If data was accidentally destroyed or was lost inadvertently (i.e., no one hacked into the system where the information resided, or stole physical data), those facts in the context of an event should bear on the likelihood that the data has fallen into the hands of an unauthorized person whose possession of the data gives rise to the risk of harm. It does not make sense to treat a minor breach that threatens little or no damage to an individual -- for example, where an online computer gaming account is hacked and a hacker gains access to a player's game achievements or where a storage company misplaces internally a storage box but re-locates it shortly thereafter -- the same way as a breach that is likely to create a significant risk of substantial harm, such as a breach involving sensitive personal data (e.g., an electronic medical record).*
- ***Finally, the amendments delete references to delegated acts.*** *Given the essential nature of breach obligations to the Union's data protection framework, the rules on breach should be addressed in the Regulation itself -- and not left to secondary rulemaking.*