19

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:56
To: Verweij, Ellen
Subject: FW: DIGITALEUROPE comments on Chapter IV of the General Data Protection Regulation
Attachments: DIGITALEUROPE comments Council text 17 Sept.pdf

Categories: Red Category

From: BRE-JUS
Sent: woensdag 24 september 2014 18:24
To: Grave, Martijn-de; Ruiter, Mieneke-de; Dam, Caroline-ten; Alink, Marnix; Kaai, Geran; Sorel, Alexander; Luijsterburg, Sander; Zwart, Jan; Kroner, Laetitia; Leenders, Sophie; Rip, Jet
Subject: FW: DIGITALEUROPE comments on Chapter IV of the General Data Protection Regulation

---

Van: [redacted]
Verzonden: woensdag 24 september 2014 18:23:32 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Aan: [redacted]
Onderwerp: DIGITALEUROPE comments on Chapter IV of the General Data Protection Regulation

Dear attaché,

We are writing you ahead of the upcoming DAPIX working group discussion on Chapter IV of the proposed General Data Protection Regulation. We would like to offer some comments, which we hope you will find helpful for the discussions you will be having and in the future.

We remain at your disposal should you wish to discuss these issues in greater detail.

Kind regards,

[redacted]
Digital Economy Policy Group

DIGITALEUROPE >> Rue de la Science, 14 >> B-1040 Brussels
T. +32 2 [redacted] >> **M.** +32 496 [redacted]
http://www.digitaleurope.org

The information in this email is confidential and is intended solely for the addressee. Access to this email by anyone else is unauthorised. If you are not the intended recipient, you must not read, use or disseminate the information. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of DIGITALEUROPE aisbl.

The information in this email is confidential and is intended solely for the addressee. Access to this email by anyone else is unauthorised. If you are not the intended recipient, you must not read, use or disseminate the information. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of DIGITALEUROPE aisbl.

Presidency text	DIGITALEUROPE proposal
60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation **(…)**. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. The likelihood and seriousness of the prejudice are determined in function of the nature, scope, context and purposes of the data processing. Risks should be evaluated on an objective assessment, by which its established whether data processing **operations involve a specific risk. A specific risk is a risk that involves a significant likelihood** of prejudice to the rights and freedoms of data subjects, **including any tangible or intangible damage, or distress.** Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular: o where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss	60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation **(…)**. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. The likelihood and seriousness of the prejudice are determined in function of the nature, scope, context and purposes of the data processing and specific risks involved. Such risks are likely to be present: ~~***Risks should be evaluated on an objective assessment, by which its established whether data processing operations involve a specific risk. A specific risk is a risk that involves a significant likelihood of prejudice to the rights and freedoms of data subjects, including any tangible or intangible damage, or distress. Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:***~~ ~~o~~ where the processing may give rise to discrimination, identity theft or fraud, ***or***

of confidentiality, **breach of anonymity or pseudonymity,** of data protected by professional secrecy, or any other significant economic or social disadvantage; or ○ where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; ○ where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; ○ where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; ○ where personal data of vulnerable individuals, in particular of children, are processed; ○ where processing involves a large amount of personal data and affects a large number of data subjects; ○ **where the data processing violates - depending on its context and the relationship between controller and data subject - the data subject's reasonable expectations.**	~~***financial loss, damage of reputation, loss of confidentiality, breach of anonymity or pseudonymity, of data protected by professional secrecy, or any other significant economic or social disadvantage; or***~~ ~~○ ***where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;***~~ ○ where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; ~~○ ***where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;***~~ ~~○ ***where personal data of vulnerable individuals, in particular of children, are processed;***~~ ~~○ ***where processing involves a large amount of personal data and affects a large number of data subjects;***~~ ~~○ ***where the data processing violates - depending on its context and the relationship between controller and data subject - the data subject's reasonable expectations.***~~

Justification:

We recommend deleting examples which are too detailed or specific as they risk being interpreted in practice as recommended cases and do not serve the purpose of a recital.

Also, the recital includes language links specific risk to the amount of data being processed. This seems contrary to the whole idea of differentiating between the processing of data that could be potentially very risky (i.e. sensitive data) and processing of data that poses not particular risk. The amount of data being processed does not necessary have an impact on the riskiness of the processing to the data subject. The recital already captures data that can be consider a specific risk, this just throws in all other data as well.

Finally, the recital includes some very subjective criteria i.e. "the data subject's reasonable expectations" – in the absence of objective criteria of what constitutes "reasonable expectations" this creates no legal certainty.

Presidency text	DIGITALEUROPE proposal
Recital 60 c) Guidance for the implementation of such measures by the controller [or processor], especially as regards the identification of the risks related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risks, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. **The European Data Protection Board may also issue guidelines on processing operations that are considered to be unlikely to result into a specific risk for the rights and freedoms of data subjects and indicate what measures may be sufficient in such cases to address such risk.** (...)	***Recital 60 c)*** Guidance for the implementation of such measures by the controller [or processor], especially as regards the identification of the risks related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risks, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. **The European Data Protection Board *shall* ~~may~~ also issue guidelines on processing operations that are considered to be unlikely to result into a specific risk for the rights and freedoms of data subjects and indicate what measures may be sufficient in such cases to address such risk.** (...)

Justification:

If it is agreed that EDPB received this responsibility then it is preferable to make it mandatory.

Presidency text	DIGITALEUROPE proposal
Recital 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	Recital 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 to ensure that the requirements of this Regulation are met. In order to be able to 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. **Such measures could consist of minimising the processing of personal data, anonymising and/or pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. Producers of the products, services and applications referred to in paragraph 1 shall be required to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.**	measures are taken to ensure that the requirements of this Regulation are met. In order to be able to 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. **Such measures could consist of minimising the processing of personal data, anonymising and/or pseudonymising personal data ~~as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing,~~ enabling the controller to create and improve security features. ~~Producers of the products, services and applications referred to in paragraph 1 shall be required to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.~~**

Justification:

We believe the term "as soon as possible" is too vague and that the reference to transparency serves no clear purpose. Moreover, we believe that access to their data does not justify the data subject monitoring data processing. Finally the last sentence is deleted since this falls under product liability rules and is not fit for data protection legislation.

Presidency text	DIGITALEUROPE proposal
Recital 63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated **also** by means of adherence of the processor to **an approved** code of conduct or **an approved**	Recital 63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, ~~***in particular in terms of expert knowledge, reliability and resources,***~~ to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated **also** by means of adherence of the processor to **an approved** code of conduct or **an approved**

certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.	certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject. ***~~The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism.~~ After the completion of the processing on behalf of the controller, the processor should return or delete the personal data.~~, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.~~***

Justification:

This is adding clauses to Article 26 which is not the purpose of the recital. Moreover, the last paragraph goes against the principle of contractual freedom.

Presidency text	DIGITALEUROPE proposal
Recital 65 In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.	Recital 65 ***~~In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.~~***

Justification:

This would incur unjustifiably high costs in practice.

Presidency text	DIGITALEUROPE proposal
Recital 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, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.	Recital 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, including confidentiality, ***as appropriate*** taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed~~***, which may in particular lead to physical, material or moral damage.***~~

Presidency text	DIGITALEUROPE proposal
Recital 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 in the Union, **and** *the processing it carries out involves a* ***specific risk*** *for the rights and freedoms of data subjects, having regard to the nature, scope,* ***context*** *and purposes of the processing* **as well as the likelihood and severity of risks for the rights and freedoms of data subjects**, the controller should designate a representative, unless **(…)** the controller is a public authority or	Recital 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 in the Union, ~~***and the processing it carries out involves a specific risk for the rights and freedoms of data subjects, having regard to the nature, scope, context and purposes of the processing as well as the likelihood and severity of risks for the rights and freedoms of data subjects,***~~ the controller should designate a representative, unless **(…)** the controller is a public

body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority.	authority or body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority.

Justification:

This would prove challenging for small app developers based outside the EU but whose service is available to EU citizens.

Presidency text	DIGITALEUROPE proposal
Recital 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, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.	Recital 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, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or ~~moral~~ damage.

Justification:

This could potentially be difficult to judge

Presidency text	DIGITALEUROPE proposal
Recital 66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to **result in a specific** risk for the rights and freedoms of data subjects, the controller [or the processor] should	Recital 66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to **result in a specific** risk for the rights and freedoms of data subjects, the controller [or the processor] should

be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, likelihood and severity of these risks. The outcome of the assessment should be taken into account when determining the (…) appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. **W**here a data protection impact assessment indicates that processing operations involve a **specific** (…) risk which **the controller** cannot mitigate by **appropriate** measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.	be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, likelihood and severity of these risks. The outcome of the assessment should be taken into account when determining the (…) appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. **W**here a data protection impact assessment indicates that processing operations involve a **specific** (…) risk which **the controller** cannot mitigate by **appropriate** measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing ***at the initiative of the controller.***

Presidency text	DIGITALEUROPE proposal
Article 25 1) Where Article 3(2) applies *and the processing* the controller *carries out* ***is likely to result in a specific*** *risk for the rights and freedoms of data subjects, having regard to the nature,* ***context****, scope and purposes of the processing*; the controller shall designate in writing a representative in the Union.	Article 25 1) Where Article 3(2) applies *and the processing* the controller *carries out* ***is likely to result in a specific*** *risk for the rights and freedoms of data subjects, having regard to the nature,* ***context****, scope and purposes of the processing*; the controller shall designate in writing a representative in the Union.

Justification:

This would prove challenging for small app developers based outside the EU but whose service is available to EU citizens. (In line with Recital 63)

Presidency text	DIGITALEUROPE proposal
Article 26 1a **The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes**.	Article 26 1a **The processor shall not enlist another processor without the prior specific or general written consent of the controller.** ~~**In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.**~~

Justification:

This paragraph should only oblige processor and controller to decide on whether and under which circumstances the processor may enlist a sub-processor – it should not prescribe how this process has to be handled.

Presidency text	DIGITALEUROPE proposal
Article 26 2) The carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, **the powers of the controller** (…) and stipulating, in particular that the processor shall:	Article 26 2) The carrying out of processing by a processor shall be governed by a contract or other legal act ~~*under*~~ ***as per*** Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, **the powers of the controller** (…) and stipulating, in particular that the processor shall:
(a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement **before processing the data**, unless that law prohibits such information on important grounds of public interest;	(a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement ~~***before processing the data,***~~ unless that law prohibits such information on important grounds of public interest;
(b) (...)	(b) (...)
(c) (...)	(c) (...)
(d) respect the conditions for enlisting another processor (…), such as a requirement of specific prior permission of the controller;	~~***(d) respect the conditions for enlisting another processor (…), such as a requirement of specific prior permission of the controller;***~~
	(ee) [NEW] enlist another processor only under conditions set by with the prior permission of the controller and to ensure all relevant provisions governing the processing of personal data by the processor are made binding on such new processors;
(e) **to the extent stipulated**, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;	(e) **to the extent stipulated *in the agreement***, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;
(f) **to the extent stipulated**, assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	(f) **to the extent stipulated *in the agreement***, assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject;	(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, ~~***unless there is a requirement to store the data under Union or Member State law to which the processor is subject;***~~
(h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article **and allow for and contribute to audits conducted by the controller.**	(h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article **and allow for and contribute to audits conducted by the controller** ***or a third party the processor and the controller agree on.***

The processor must immediately inform the controller if, in his opinion, an instruction breaches data protection rules.	**The processor must ~~immediately~~ *upon discovery* inform the controller if, in his opinion, an instruction breaches data protection rules.**

Justification:

A duty to inform before processing is unrealistic: Problems can only be identified during the actual processing.

Moreover, 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. For example, a controller may want to ensure that additional sub-processors - which may be numerous – apply effective data protection. But it should be clear this does not mean they should assess each in turn prior to their employment. As the processor has the closer relationship, they are better placed to make such a judgment. 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. 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. Finally, Art 26(4) implies that the controller would need to provide very detailed instructions as to what personal data the processor shall process. In reality, this is often not the case, yet based on this article the processor would carry the liability for not receiving extremely detailed instructions from the controller. Where a processor does breach such instructions, it is logical that the processor is considered a controller in respect of that processing but there is no reason to include the original data controller as a joint controller in this instance.

Note: paragraph 2 could be in breach of the principle of freedom of contracting.

Presidency text	DIGITALEUROPE proposal
Article 26 2a) Where a processor enlists **(...)** another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor *by way of a contract or other legal act under Union or Member State law,* in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Article 26 2a) Where a processor enlists **(...)** another processor for carrying out specific processing activities on behalf of the controller, the ~~***same***~~ ***relevant*** data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor *by way of a contract or other legal act under Union or Member State law,* in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the ***relevant*** requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Presidency text	DIGITALEUROPE proposal
Article 26 2ab) Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.	Article 26 2ab) ***~~Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.~~***

Presidency text	DIGITALEUROPE proposal
Article 26 2b) The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2).	Article 26 2b) ***~~The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2).~~***

Presidency text	DIGITALEUROPE proposal
Article 26 2c) A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.	Article 26 2c) ***~~A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.~~***

Justification for Articles 26 2ab), 2b) and 2c):

These clauses are in breach of the contractual freedom principle.

Presidency text	DIGITALEUROPE proposal
Article 26 3) The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.	Article 26 3) ***~~The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.~~***

Justification:

These clauses are in breach of some national legal traditions. (e.g French civil code)

Presidency text	DIGITALEUROPE proposal
Article 28 2a) a	Article 28 2a) a
Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the categories of processing carried out on behalf of each controller;	Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing: ~~***(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;***~~ (b) the name and contact details of the data protection officer, if any; ~~***(c) the categories of processing carried out on behalf of each controller;***~~

Justification:

We believe this would already be captured by the contract with the controller or sub-processor and is therefore an unnecessary duplication.

Presidency text	DIGITALEUROPE proposal
Article 31 1)	Article 31 1)
In the case of a personal data breach which is likely to **result in** a **specific** risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, **breach of anonymity or pseudonymity,** damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.	In the case of a personal data breach which is likely to **result in** a **specific** risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, **breach of anonymity or pseudonymity,** damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay ~~***and, where feasible, not later than 72 hours after having become aware of it,***~~ notify the personal data breach to the supervisory authority competent in accordance with Article 51. ~~***The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.***~~

Justification:

We warmly welcome that the Presidency text introduces a materiality threshold as to what types of personal data breaches should be notified. At the same time, we regret that the Presidency text does not state that breaches should be notified without 'undue delay'. We firmly believe that the notification deadline should be flexible enough to reflect the different degrees of complexity in identifying the nature and scope of a breach depending on the breach in question and so as not to interrupt a company's efforts to deal with the breach and withstand sustained attacks (which could actually lead to further breaches).

Presidency text	DIGITALEUROPE proposal
Article 31 1a) 1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b).	Article 31 1a) 1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b).

DIGITALEUROPE would like to stress that this paragraph should be retained.

Presidency text	DIGITALEUROPE proposal
Article 31 5) **Pursuant to Union law or the law of a Member State the competent supervisory authority shall inform the national information security authorities without undue delay about the data breach.**	Article 31 5) **Pursuant to Union law or the law of a Member State the competent supervisory authority shall inform the national information security authorities without undue delay about the data breach.**

DIGITALEUROPE would like to point out that this obligation should depend on the nature of the breach, i.e. if the breach was due to a security flaw.

Presidency text	DIGITALEUROPE proposal
Article 33 dd) **processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where reasonable expectations are not met, for example owing to the context of the processing operation;**	Article 33 dd) **processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, ~~where a new technology is used,~~ where it is more difficult for data subjects to exercise their rights, ~~or where reasonable expectations are not met,~~ for example owing to the context of the processing operation;**

Justification:

Technology should be treated the same regardless of whether new or not. This does not promote innovation.

The term “reasonable expectations” is legally uncertain.

Presidency text	DIGITALEUROPE proposal
Article 33 2a) The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	Article 33 2a) ~~**The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.**~~

Justification:

This would let individual DPAs specify broad categories of processing that will require prior consultation and therefore undermine the basic principle of the same law applying cross the board.

Presidency text	DIGITALEUROPE proposal
Article 33 2b) **The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board**.	Article 33 2b) **The supervisory authority ~~may~~ shall also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board**.

The term "shall" avoids one-way traffic

Presidency text	DIGITALEUROPE proposal
Article 34 Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where **the controller has** insufficiently identified or mitigated *the risk*, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller **, in writing, and may prohibit the processing pursuant to Article 53, paragraph 1b, letter e**). This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.	Article 34 Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where **the controller has** insufficiently identified or mitigated *the risk*, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller **, in writing, and may prohibit the processing pursuant to Article 53, paragraph 1b, letter e**). This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.

DIGITALEUROPE asks for a reduction of the time period. This seems very long and does not match the innovation timescale – it can take up to 3 months until a consultation is responded to.

Comments to Council text dated 17 September 2014

Presidency text	DIGITALEUROPE proposal
60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation **(…)**. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. The likelihood and seriousness of the prejudice are determined in function of the nature, scope, context and purposes of the data processing. Risks should be evaluated on an objective assessment, by which its established whether data processing **operations involve a specific risk. A specific risk is a risk that involves a significant likelihood** of prejudice to the rights and freedoms of data subjects, **including any tangible or intangible damage, or distress.** Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular: o where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss	60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation **(…)**. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. The likelihood and seriousness of the prejudice are determined in function of the nature, scope, context and purposes of the data processing and specific risks involved. Such risks are likely to be present: ~~***Risks should be evaluated on an objective assessment, by which its established whether data processing operations involve a specific risk. A specific risk is a risk that involves a significant likelihood of prejudice to the rights and freedoms of data subjects, including any tangible or intangible damage, or distress. Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:***~~ ~~o~~ where the processing may give rise to discrimination, identity theft or fraud, ***or***

of confidentiality, **breach of anonymity or pseudonymity,** of data protected by professional secrecy, or any other significant economic or social disadvantage; or ○ where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; ○ where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; ○ where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; ○ where personal data of vulnerable individuals, in particular of children, are processed; ○ where processing involves a large amount of personal data and affects a large number of data subjects; ○ **where the data processing violates - depending on its context and the relationship between controller and data subject - the data subject's reasonable expectations.**	~~***financial loss, damage of reputation, loss of confidentiality, breach of anonymity or pseudonymity, of data protected by professional secrecy, or any other significant economic or social disadvantage; or***~~ ~~○ ***where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;***~~ ○ where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; ~~○ ***where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;***~~ ~~○ ***where personal data of vulnerable individuals, in particular of children, are processed;***~~ ~~○ ***where processing involves a large amount of personal data and affects a large number of data subjects;***~~ ~~○ ***where the data processing violates - depending on its context and the relationship between controller and data subject - the data subject's reasonable expectations.***~~

Justification:

We recommend deleting examples which are too detailed or specific as they risk being interpreted in practice as recommended cases and do not serve the purpose of a recital.

Also, the recital includes language links specific risk to the amount of data being processed. This seems contrary to the whole idea of differentiating between the processing of data that could be potentially very risky (i.e. sensitive data) and processing of data that poses not particular risk. The amount of data being processed does not necessary have an impact on the riskiness of the processing to the data subject. The recital already captures data that can be consider a specific risk, this just throws in all other data as well.

Finally, the recital includes some very subjective criteria i.e. “the data subject’s reasonable expectations” – in the absence of objective criteria of what constitutes “reasonable expectations” this creates no legal certainty.

Presidency text	DIGITALEUROPE proposal
Recital 60 c) Guidance for the implementation of such measures by the controller [or processor], especially as regards the identification of the risks related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risks, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. **The European Data Protection Board may also issue guidelines on processing operations that are considered to be unlikely to result into a specific risk for the rights and freedoms of data subjects and indicate what measures may be sufficient in such cases to address such risk.** (…)	***Recital 60 c)*** Guidance for the implementation of such measures by the controller [or processor], especially as regards the identification of the risks related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risks, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. **The European Data Protection Board *shall* ~~may~~ also issue guidelines on processing operations that are considered to be unlikely to result into a specific risk for the rights and freedoms of data subjects and indicate what measures may be sufficient in such cases to address such risk.** (…)

Justification:

If it is agreed that EDPB received this responsibility then it is preferable to make it mandatory.

Presidency text	DIGITALEUROPE proposal
Recital 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	Recital 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 to ensure that the requirements of this Regulation are met. In order to be able to 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. **Such measures could consist of minimising the processing of personal data, anonymising and/or pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. Producers of the products, services and applications referred to in paragraph 1 shall be required to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.**	measures are taken to ensure that the requirements of this Regulation are met. In order to be able to 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. **Such measures could consist of minimising the processing of personal data, anonymising and/or pseudonymising personal data ~~as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing,~~ enabling the controller to create and improve security features. ~~Producers of the products, services and applications referred to in paragraph 1 shall be required to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.~~**

Justification:

We believe the term "as soon as possible" is too vague and that the reference to transparency serves no clear purpose. Moreover, we believe that access to their data does not justify the data subject monitoring data processing. Finally the last sentence is deleted since this falls under product liability rules and is not fit for data protection legislation.

Presidency text	DIGITALEUROPE proposal
Recital 63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated **also** by means of adherence of the processor to **an approved** code of conduct or **an approved**	Recital 63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, ~~***in particular in terms of expert knowledge, reliability and resources,***~~ to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Such sufficient guarantees may be demonstrated **also** by means of adherence of the processor to **an approved** code of conduct or **an approved**

certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.	certification mechanism. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risks for the rights and freedoms of the data subject. ***~~The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism.~~ After the completion of the processing on behalf of the controller, the processor should return or delete the personal data.~~, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.~~***

Justification:

This is adding clauses to Article 26 which is not the purpose of the recital. Moreover, the last paragraph goes against the principle of contractual freedom.

Presidency text	DIGITALEUROPE proposal
Recital 65 In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.	Recital 65 ***~~In order to demonstrate compliance with this Regulation, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.~~***

Justification:

This would incur unjustifiably high costs in practice.

Presidency text	DIGITALEUROPE proposal
Recital 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, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.	Recital 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, including confidentiality, ***as appropriate*** taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed~~***, which may in particular lead to physical, material or moral damage.***~~

Presidency text	DIGITALEUROPE proposal
Recital 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 in the Union, **and** *the processing it carries out involves a* ***specific risk*** *for the rights and freedoms of data subjects, having regard to the nature, scope,* ***context*** *and purposes of the processing* **as well as the likelihood and severity of risks for the rights and freedoms of data subjects**, the controller should designate a representative, unless **(…)** the controller is a public authority or	Recital 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 in the Union, ~~***and the processing it carries out involves a specific risk for the rights and freedoms of data subjects, having regard to the nature, scope, context and purposes of the processing as well as the likelihood and severity of risks for the rights and freedoms of data subjects,***~~ the controller should designate a representative, unless **(…)** the controller is a public

body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority.	authority or body (…). The representative should act on behalf of the controller and may be addressed by any supervisory authority.

Justification:

This would prove challenging for small app developers based outside the EU but whose service is available to EU citizens.

Presidency text	DIGITALEUROPE proposal
Recital 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, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.	Recital 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, including confidentiality, taking into account available technology and the costs of (…) implementation in relation to the risks and the nature of the personal data to be protected. (…). In assessing data security risks, consideration should be given **to the** given risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or ~~*moral*~~ damage.

Justification:

This could potentially be difficult to judge

Presidency text	DIGITALEUROPE proposal
Recital 66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to **result in a specific** risk for the rights and freedoms of data subjects, the controller [or the processor] should	Recital 66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to **result in a specific** risk for the rights and freedoms of data subjects, the controller [or the processor] should

be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, likelihood and severity of these risks. The outcome of the assessment should be taken into account when determining the (...) appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. **Where** a data protection impact assessment indicates that processing operations involve a **specific** (...) risk which **the controller** cannot mitigate by **appropriate** measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.	be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, likelihood and severity of these risks. The outcome of the assessment should be taken into account when determining the (...) appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. **Where** a data protection impact assessment indicates that processing operations involve a **specific** (...) risk which **the controller** cannot mitigate by **appropriate** measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing ***at the initiative of the controller.***

Presidency text	DIGITALEUROPE proposal
Article 25 1) Where Article 3(2) applies *and the processing* the controller *carries out* ***is likely to result in a specific*** *risk for the rights and freedoms of data subjects, having regard to the nature,* ***context****, scope and purposes of the processing*; the controller shall designate in writing a representative in the Union.	Article 25 1) Where Article 3(2) applies *and the processing* the controller *carries out* ***is likely to result in a specific*** *risk for the rights and freedoms of data subjects, having regard to the nature,* ***context****, scope and purposes of the processing*; the controller shall designate in writing a representative in the Union.

Justification:

This would prove challenging for small app developers based outside the EU but whose service is available to EU citizens. (In line with Recital 63)

Presidency text	DIGITALEUROPE proposal
Article 26 1a **The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes**.	Article 26 1a **The processor shall not enlist another processor without the prior specific or general written consent of the controller.** ~~*In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.*~~

Justification:

This paragraph should only oblige processor and controller to decide on whether and under which circumstances the processor may enlist a sub-processor – it should not prescribe how this process has to be handled.

Presidency text	DIGITALEUROPE proposal
Article 26 2)	Article 26 2)
The carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, **the powers of the controller** (…) and stipulating, in particular that the processor shall:	The carrying out of processing by a processor shall be governed by a contract or other legal act ***~~under~~ as per*** Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, **the powers of the controller** (…) and stipulating, in particular that the processor shall:
(a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement **before processing the data**, unless that law prohibits such information on important grounds of public interest;	(a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement ***~~before processing the data,~~*** unless that law prohibits such information on important grounds of public interest;
(b) (...)	(b) (...)
(c) (...)	(c) (...)
(d) respect the conditions for enlisting another processor (…), such as a requirement of specific prior permission of the controller;	***~~(d) respect the conditions for enlisting another processor (…), such as a requirement of specific prior permission of the controller;~~***
	(ee) [NEW] enlist another processor only under conditions set by with the prior permission of the controller and to ensure all relevant provisions governing the processing of personal data by the processor are made binding on such new processors;
(e) **to the extent stipulated**, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;	(e) **to the extent stipulated *in the agreement***, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;
(f) **to the extent stipulated**, assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	(f) **to the extent stipulated *in the agreement***, assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject;	(g) return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, ***~~unless there is a requirement to store the data under Union or Member State law to which the processor is subject;~~***
(h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article **and allow for and contribute to audits conducted by the controller.**	(h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article **and allow for and contribute to audits conducted by the controller *or a third party the processor and the controller agree on.***

The processor must immediately inform the controller if, in his opinion, an instruction breaches data protection rules.	**The processor must ~~immediately~~ *upon discovery* inform the controller if, in his opinion, an instruction breaches data protection rules.**

Justification:

A duty to inform before processing is unrealistic: Problems can only be identified during the actual processing.

Moreover, 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. For example, a controller may want to ensure that additional sub-processors - which may be numerous – apply effective data protection. But it should be clear this does not mean they should assess each in turn prior to their employment. As the processor has the closer relationship, they are better placed to make such a judgment. 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. 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. Finally, Art 26(4) implies that the controller would need to provide very detailed instructions as to what personal data the processor shall process. In reality, this is often not the case, yet based on this article the processor would carry the liability for not receiving extremely detailed instructions from the controller. Where a processor does breach such instructions, it is logical that the processor is considered a controller in respect of that processing but there is no reason to include the original data controller as a joint controller in this instance.

Note: paragraph 2 could be in breach of the principle of freedom of contracting.

Presidency text	DIGITALEUROPE proposal
Article 26 2a) Where a processor enlists **(...)** another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor *by way of a contract or other legal act under Union or Member State law*, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Article 26 2a) Where a processor enlists **(...)** another processor for carrying out specific processing activities on behalf of the controller, the ~~***same***~~ ***relevant*** data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 2 shall be imposed on that other processor *by way of a contract or other legal act under Union or Member State law*, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the ***relevant*** requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Presidency text	DIGITALEUROPE proposal
Article 26 2ab) Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.	Article 26 2ab) ~~***Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.***~~

Presidency text	DIGITALEUROPE proposal
Article 26 2b) The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2).	Article 26 2b) ~~***The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2).***~~

Presidency text	DIGITALEUROPE proposal
Article 26 2c) A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.	Article 26 2c) ~~***A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.***~~

Justification for Articles 26 2ab), 2b) and 2c):

These clauses are in breach of the contractual freedom principle.

Presidency text	DIGITALEUROPE proposal
Article 26 3) The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.	Article 26 3) ~~***The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.***~~

Justification:

These clauses are in breach of some national legal traditions. (e.g French civil code)

Presidency text	DIGITALEUROPE proposal
Article 28 2a) a Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the categories of processing carried out on behalf of each controller;	Article 28 2a) a Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing: ~~***(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;***~~ (b) the name and contact details of the data protection officer, if any; ~~***(c) the categories of processing carried out on behalf of each controller;***~~

Justification:

We believe this would already be captured by the contract with the controller or sub-processor and is therefore an unnecessary duplication.

Presidency text	DIGITALEUROPE proposal
Article 31 1) In the case of a personal data breach which is likely to **result in a specific** risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, **breach of anonymity or pseudonymity,** damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.	Article 31 1) In the case of a personal data breach which is likely to **result in a specific** risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, **breach of anonymity or pseudonymity,** damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay ~~***and, where feasible, not later than 72 hours after having become aware of it,***~~ notify the personal data breach to the supervisory authority competent in accordance with Article 51. ~~***The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.***~~

Justification:

We warmly welcome that the Presidency text introduces a materiality threshold as to what types of personal data breaches should be notified. At the same time, we regret that the Presidency text does not state that breaches should be notified without 'undue delay'. We firmly believe that the notification deadline should be flexible enough to reflect the different degrees of complexity in identifying the nature and scope of a breach depending on the breach in question and so as not to interrupt a company's efforts to deal with the breach and withstand sustained attacks (which could actually lead to further breaches).

Presidency text	DIGITALEUROPE proposal
Article 31 1a) 1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b).	Article 31 1a) 1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b).

DIGITALEUROPE would like to stress that this paragraph should be retained.

Presidency text	DIGITALEUROPE proposal
Article 31 5) **Pursuant to Union law or the law of a Member State the competent supervisory authority shall inform the national information security authorities without undue delay about the data breach.**	Article 31 5) **Pursuant to Union law or the law of a Member State the competent supervisory authority shall inform the national information security authorities without undue delay about the data breach.**

DIGITALEUROPE would like to point out that this obligation should depend on the nature of the breach, i.e. if the breach was due to a security flaw.

Presidency text	DIGITALEUROPE proposal
Article 33 dd) **processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where reasonable expectations are not met, for example owing to the context of the processing operation;**	Article 33 dd) **processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, ~~where a new technology is used,~~ where it is more difficult for data subjects to exercise their rights, ~~or where reasonable expectations are not met,~~ for example owing to the context of the processing operation;**

Justification:

Technology should be treated the same regardless of whether new or not. This does not promote innovation.

The term "reasonable expectations" is legally uncertain.

Presidency text	DIGITALEUROPE proposal
Article 33 2a) The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	Article 33 2a) ~~**The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.**~~

Justification:

This would let individual DPAs specify broad categories of processing that will require prior consultation and therefore undermine the basic principle of the same law applying cross the board.

Presidency text	DIGITALEUROPE proposal
Article 33 2b) **The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.**	Article 33 2b) **The supervisory authority ~~may~~ shall also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.**

The term "shall" avoids one-way traffic

Presidency text	DIGITALEUROPE proposal
Article 34 Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where **the controller has** insufficiently identified or mitigated *the risk*, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller **, in writing, and may prohibit the processing pursuant to Article 53, paragraph 1b, letter e**). This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.	Article 34 Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where **the controller has** insufficiently identified or mitigated *the risk*, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller **, in writing, and may prohibit the processing pursuant to Article 53, paragraph 1b, letter e**). This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.

DIGITALEUROPE asks for a reduction of the time period. This seems very long and does not match the innovation timescale – it can take up to 3 months until a consultation is responded to.