Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission's proposal for a General Data Protection Regulation "on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

1. Jurisdiction/One-stop shop/Consistency mechanism

The core principle of a single Data Protection Authority (DPA) having jurisdiction over organisations that operate across multiple European countries is a sensible and positive development in the draft Regulation. The 'one-stop shop' principle has the potential of creating the right incentives for international organisations to establish and invest in Europe. However there are some aspects of the drafting of the draft Regulation which need to be improved if this principle is to be realised. This will in turn provide better protection for European citizens who will be able to seek redress in the European Union (the "EU").

In particular, for citizens and international organisations with a presence in the EU to reap the full benefits of the one-stop shop principle, it must be clear how the law applies in the case of group companies. Where if there is already an EU based controller within a corporate group, that controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority.

Further, many provisions of the draft Regulation undermine the intent of the one-stop shop principle and create legal uncertainty for businesses. These provisions should be revised to maintain the robustness of the changes that are proposed.

<u>Drafting recommendations</u>:

Article 3 (Territorial scope): If there is already an EU-based controller processing the same personal data as a non-EU based controller within a corporate group, the EU-based controller should be responsible for compliance in respect of the relevant data processing (as per Article 3(1)).

As further explained in section 4 "profiling" of this document, the draft Regulation as it is currently worded is set to apply to non-EU controllers when the processing relates to the 'monitoring of an individual's behaviour'. It is our view that the express reference to 'monitoring' undermines the principle of technology neutrality. *Article 55 (Mutual Assistance):* The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities. We therefore propose:

- deleting the mutual assistance obligations regarding prior authorisations (Article 55(1)) and the ability to take a provisional measure and submit the matter the EDPB where a request for assistance is not actioned within 1 month (Article 55(8) and (9));

- the measures required to reply to a request of another supervisory authority must be "reasonable". Further, requests made by another supervisory authority for general "enforcement measures" should be specifically limited to requests for the communication of any enforcement decision which relates to processing operations that have been proven to be contrary to the Regulation (Article 55(2)).

- the mutual assistance provisions should only apply:

  - where individuals in several member states are likely to be affected by the processing to operations that "produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect them in a significantly negative manner" (Article 55(1));

  - unless complying with request for assistance would "involve disproportionate effort" (Article 55(4)(b)).

Article 58 (Consistency Mechanism - Opinion by the European Data Protection Board): The consistency mechanism should only apply in limited circumstances to avoid a potentially massive and damaging bureaucratisation of the decision making process by the data protection authorities.

Drafting suggestions:

Recital 27 The main establishment of a controller or a processor 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.	Recital 27 The main establishment of a controller ~~*or a processor*~~ 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.***

Justification
Retain the European Commission's text. The proposed additions do not work given the different definitions between controller and processor in the draft Regulation.

Recital 97 (EC proposal)	Recital 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.	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.
Justification The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller.	

Recital 105	Recital 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	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*~~ ***the competent*** supervisory authority intends to take a measure as

operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring ***of*** such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism***. Furthermore, the data subjects should have the right to obtain consistency, if they deem a measure by a Data Protection Authority of a Member State has not fulfilled this criterion***. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.	regards processing operations that are related to ***the fundamental rights and freedoms of a data subject*** ~~*the offering of goods or services to data subjects in several Member States, or to the monitoring of such data subjects*~~, or that might substantially affect the free flow of personal data. It should also apply where ***those factors are present and*** 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.
Justification The consistency mechanism should only apply in limited circumstances (and where there is a substantial public interest) to avoid a potentially massive and very damaging bureaucratisation of the decision making process by the data protection authorities. The range of instances that trigger that mechanism, the ability of the Commission to launch it, and the process to be followed need to be carefully worded so that they can reflect the practical viability and resources required. References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51. Further, the express reference to 'monitoring' violates the principle of technology neutrality. In any event, any adverse effects to the data subject that may result from the 'monitoring of an individual's behavior' are already adequately protected by the provisions of this regulation.	

Recital 108 (EC proposal) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified	Recital 108 There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, ~~*a*~~ ***the competent*** supervisory authority should be able to adopt provisional measures with a

period of validity when applying the consistency mechanism	specified period of validity when applying the consistency mechanism.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Recital 109 (EC proposal) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.	Recital 109 The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by ~~*a*~~ ***the competent*** supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Recital 111 Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject. ***If the data subject deems consistency is not fulfilled, a complaint to the European Data Protection Board can be filed***	Recital 111 Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject. ~~*If the data subject deems consistency is not fulfilled, a complaint to the European Data Protection Board can be filed.*~~
Justification Retain the European Commission's text. It is unclear what power the European Data Protection Board (the 'EDPB') has in such a situation. If an opinion is issued, the draft Regulation does not empower the EDPB to force a supervisory authority to abide by that	

opinion. Such powers should ultimately lie with the courts, not the EDPB.

Recital 113 Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established***, or before the European Data Protection Board on grounds of inconsistency with the application of the present Regulation in other Member States***	Recital 113 Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established***.***
Justification Retain the European Commission's text. It is unclear what power the European Data Protection Board (the 'EDPB') has in such a situation. If an opinion is issued, the draft Regulation does not empower the EDPB to force a supervisory authority to abide by that opinion. Such powers should ultimately lie with the courts, not the EDPB.	

Article 3 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 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 ***and*** services to such data subjects in the Union***, including services provided without financial costs to the individual, or;*** (b) the monitoring of their behaviour. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place	Article 3 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 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~~ ***except where the processing of personal data is carried out by a controller within the same corporate group of a controller to which paragraph 1 applies.***

where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law..
Justification The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller. Any adverse effects to the data subject that may result from the 'monitoring of an individual's behavior' is adequately covered by the provisions of this regulation. It is unclear why an express reference to this should be made under the territorial scope provisions – such reference could jeopardise the technologically neutral nature of the proposal.	

Article 4(1)(13) 'main establishment' means ***the place where*** the controller ***or the processor has*** 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 ***or a processor*** in the Union take place.	Article 4(1)(13) 'main establishment' means ***as regards*** ~~*the place where*~~ the controller, ***the place of*** ~~*or the processor has*~~ 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 ~~*or a processor*~~ in the Union take place. ***As regards the processor, 'main establishment' means the place of its central administration in the Union;***
Justification	

Retain the European Commission's text. The proposed additions do not work given the different definitions between controller and processor in the draft Regulation.

	Article 4(1)(20)new ***'competent supervisory authority' means the supervisory authority of the controller in accordance with the Article 51(2) &(3)***
Justification 'Competent supervisory authority' should be clearly defined to assist with certainty as to which supervisory authority will have authority to supervise a controller. Further, the reference to 'competent' reinforces one of the key principles of the Regulation that one single authority will be competent in respect of the scrutiny of the controller, even if the other supervisory authorities can play a role in terms of safeguarding the data subjects within their jurisdictions.	

Article 51 (EC proposal) 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.	Article 51 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller ~~*or a processor*~~ in the Union, ***and the activities of a controller within the same corporate group not established in the Union or where*** the controller ~~or processor~~ is established in more than one Member State, the supervisory authority of the main establishment of the controller ~~or processor~~ shall be competent for the supervision of the processing activities~~*of the controller or the processor in all Member States, without prejudice to*~~ the provisions of Chapter VII of this Regulation. ***All references to the competent supervisory authority shall be***

	interpreted in accordance with this Article 51(2).
3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	4. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Justification

The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller.

'Competent supervisory authority should be clearly defined to assist with certainty as to which supervisory authority will have authority to supervise a controller. Further. the reference to competent reinforces one of the key principles of the Regulation that one single authority will be competent in respect of the scrutiny of the controller, even if the other supervisory authorities can play a role in terms of safeguarding the data subjects within their jurisdictions.

Processors should not be subject to the same administrative obligations and regulatory scrutiny as controllers as per our position in relation to Recital 65 / Article 28 (Documentation) / Article 9.

Article 55 (EC proposal)	Article 55
1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data	1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out ~~*prior authorisations and*~~ consultations, inspections and prompt information on the opening of cases and ensuing developments where data

subjects in several Member States are likely to be affected by processing operations.	subjects in several Member States are likely to be affected by processing operations ***that produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect them in a significantly negative manner;***
2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.	2. Each supervisory authority shall take all ~~*appropriate*~~ ***reasonable*** measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or ~~*enforcement measures*~~ ***communicating any enforcement decision taken*** to bring about the cessation or prohibition of processing operations ***that have been proven*** contrary to this Regulation.
3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.	3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.
4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless: (a) it is not competent for the request; or (b) compliance with the request would be incompatible with the provisions of this Regulation.	4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless: (a) it is not competent for the request; or (b) compliance with the request would be incompatible with the provisions of this Regulation ***or would involve disproportionate effort.***
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.	5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.
	6. Supervisory authorities shall supply the

6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format. 7. No fee shall be charged for any action taken following a request for mutual assistance. 8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57. 9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission. 10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format. 7. No fee shall be charged for any action taken following a request for mutual assistance. ~~*8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.*~~ ~~*9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.*~~ 10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
Justification The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities.	

Article 58 (EC proposal)	Article 58
1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.	1. Before ~~*a*~~ ***the competent*** supervisory authority adopts a measure referred to in paragraph 2, this ***competent*** supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.
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 ***concerning the fundamental rights and freedoms of a data subject*** 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 which are ***likely to produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect the individual in a significantly negative manner*** ~~*related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour*~~; 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; or
(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or	~~*(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or*~~
(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) aims to approve binding corporate rules within the meaning of Article 43.
3. Any supervisory authority or the	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.	European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism~~, in particular~~ where ~~a~~ ***the competent*** 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. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter ***related to the category of measures referred to in paragraph 2*** shall be dealt with in the consistency mechanism.
5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.	5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.
6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.	6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.
7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The	7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The

opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public. 8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.	opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the ***competent*** supervisory authority ~~*competent under Article 51*~~ of the opinion and make it public. 8. ~~*The supervisory authority referred to in paragraph 1 and t*~~***T***he ***competent*** supervisory authority ~~*competent under Article 51*~~ shall take ***utmost*** account of***, but not be bound by,*** the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.
Justification The consistency mechanism should only apply in limited circumstances to avoid a potentially massive and very damaging bureaucratisation of the decision making process by the data protection authorities. The range of instances that trigger that mechanism (paragraph 2), the ability of the Commission to launch it (paragraph 4), and the process to be followed (paragraphs 7 and 8) need to be carefully worded so that they can reflect the practical viability and resources required. With regard to the process to be followed, experience shows that despite their best efforts, supervisory authorities are not organized and resourced in a way that allows them to meet strict timeframes. Therefore, it is very likely that the timeframes set out will be routinely missed and, as a result, any decisions or measures subject to the consistency mechanism will be unnecessarily and unjustifiably delayed. In view of this, the consistency mechanism should only be engaged in a minority of situations and where there is a substantial public interest.	

Article 59 (EC proposal)	Article 59

1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.	1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.
2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.	2. Where the Commission has adopted an opinion in accordance with paragraph 1, the ***competent*** supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.
3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.	3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.
4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.	4. Where the ***competent*** supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Article 60 (EC proposal) 1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned	***delete***

decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to: (a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or (b) adopt a measure pursuant to point (a) of Article 62(1). 2. The Commission shall specify the duration of the suspension which shall not exceed 12 months. 3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.	
Justification The power granted to the European Commission to adopt interpretive opinions and draft measures undermines the principle of independent data protection supervision. Such powers should lie with the data protection supervisory authorities and ultimately the courts, not the Commission. Where an issue arises in relation to an opinion or draft measure issued by the European Data Protection Board (under Article 58) this would be most appropriately dealt with by the European Court of Justice whose primary function is to interpret the law, rather than the Commission.	

Article 61 (EC proposal)	Article 61
1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the	1. In exceptional circumstances, where ~~a~~ ***the competent*** supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way

procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.	of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The ***competent*** supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.	2. Where a ***competent*** supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.
3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.	3. Any supervisory authority may request an urgent opinion ***of the European Data Protection Board*** where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.
4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51. The specific reference to the European Data Protection Board creates certainty about the relevant body that the Supervisory authority can submit a request for an urgent opinion to.	

Article 63 (EC proposal)	Article 63
1. For the purposes of this Regulation, an enforceable measure of the supervisory	1. For the purposes of this Regulation, an enforceable measure of the ***competent***

authority of one Member State shall be enforced in all Member States concerned. 2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.	supervisory authority of one Member State shall be enforced in all Member States concerned. 2. Where a ***competent*** supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the ***competent*** supervisory authority shall not be legally valid and enforceable.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Article 63a new Appealing procedures Without prejudice to the competences of the judiciary system of the Member States and of the Union, the European Data Protection Board can issue binding opinions if: (a) a data subject or data controller appeals on ground of inconsistent application of the present Regulation across the Member States and (b) the Consistency Mechanism described in Article 58 to 63 has failed to ensure that a simple majority of the members of the European Data Protection Board agrees on a measure. Before issuing such opinion, the European Data Protection Board shall take into consideration every information the competent Data Protection Authority knows, including the point of view of the interested parties.	***delete***
Justification The EDPB should not be granted the power to adopt binding opinions. The primary function of interpreting the law should lie with the data protection supervisory authorities and ultimately the European Court of Justice whose primary function is to	

interpret the law.

Article 66(1)(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57 ***and in Article 63a***;	Article 66(1)(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57 ~~*and in Article 63a*~~;
Justification This amendment relates to the proposed new Article 63(a) above.	

Article 73(2) Any body, organisation or association which aims to protect ***citizens***' rights and interests shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.	Article 73(2) Any body, organisation or association which aims to protect ***data subjects***' ~~*citizens'*~~ rights and interests ***concerning the protection of their personal data and has been properly constituted according to the law of a Member State*** shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.
Justification The reference to 'citizen' rights' is inconsistent with the draft Regulation which refers to 'data subjects' throughout. Further, it creates a suggestion that consumer organisations or claim foundations could bundle claims of consumers and class action could be used by some as a mechanism to litigate against corporate groups. The potential scale of such collective actions, time, cost and outcome - on top of penalties - might have severe financial implications for companies. The effect of this judicial remedy would be disproportionate to the aims of deterrence and effective enforcement of the data protection provisions in the proposed Regulation.	

2. Consent

Individuals should be able to exercise control over what personal data organisations collect from them and how they use it, but the highly prescriptive nature of the requirements for consent contained in Articles 4(8) and 7(2) could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk

of inundating users with tick boxes and warnings and may result in an overly disrupted or disjointed internet experience. This will inevitably lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it. It may also prevent organisations from being innovative about the way they interact with individuals.

Unambiguous consent should be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (…) when the actions lead to an unmistakable conclusion that consent is given".

It is important to keep in mind that there are many services, such as social networks, which are expressly designed for people to be able to connect and share information.

A great amount of privacy best practice has been developed, especially in the online environment, to provide users with transparency and control. We are seeing great innovation (including granular and sophisticated control tools) from many players in the market to empower users to understand how their information is used and how services work when they choose to share information online. Equally many internet players are incorporating 'privacy by design' into their privacy programmes. These practices must not be hampered by over-prescriptive and often meaningless consent requirements.

Drafting recommendations:

Recital 25, Article 4(8) (Definition of Consent): The reference "explicit" in the definition of consent is counterproductive and unrealistic in the majority of processing situations. We therefore propose that the reference that consent must be given "explicitly" and "silence and inactivity should not constitute consent" should be deleted from Recital 25. We have suggested language that makes clear that "other conduct that leads to an unmistakable conclusion that consent is given" is valid consent. We also recommend that there should be some flexibility in the way that this is provided i.e. "either by a statement or by a clear affirmative action or by any other method" (see Recital 25 and the definition of Consent contained in Article 4(8)).

The controller is in the best position to decide the appropriate level of information to provide individuals about specific processing activities. Therefore, we propose adding wording to Article 4(8) to state that the information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles (as contained in Article 5).

Article 7 (Conditions for Consent): We propose that:

- The controller should only bear the 'burden of proof' in cases where the need for consent is in connection with the processing of sensitive personal data. This position is reflected in the proposed changes to Article 7(1).

- The Regulation shall provide common and practical examples of how processing activities can be communicated to individuals for the purposes of obtaining consent for a range of activities in a single step. This position is reflected in the proposed changes to Recital 32 and Article 7(2).

- Controllers should not be obliged to continue to offer services where individuals decline to provide their personal data. We have therefore suggested that the controller shall be entitled to suspend or terminate services where such provision of services relies on consent to the processing which has been withdrawn by the individual (see Article 7(3)).

- Controllers should be able to make consent to the processing a condition of access to a service which may not be otherwise free. This position is reflected in our amendments to Recital 34 and Article 7(4).

Drafting suggestions:

Recital 25 (EC proposal)	Recital 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	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, ***by taking some other conduct that leads to an unmistakable conclusion that consent is given***, ensuring that individuals are aware that they give their consent to the processing of personal data ~~*including by ticking a box.*~~ ***Consent may be given*** by taking an action 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

provided.	must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Justification

Unambiguous consent shall be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (…) when the actions lead to an unmistakable conclusion that consent is given".

Individuals should be able to exercise control over what personal data organisations collect from them and how they use it, but the proposed requirement for consent may lead to an overly disrupted or disjoined internet experience and may also prevent organisations from being innovative about the way they interact with individuals.

The highly prescriptive nature of the requirements for consent could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk of inundating users with tick boxes and warnings. As well as affecting the user experience, this inevitably will lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it.

Furthermore, controllers should be allowed some technical flexibility as to the way that data subjects' consent is obtained.

Recital 32 (EC proposal)	Recital 32
Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.	Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given, ***including by identifying and explaining the relevant data processing activities in a data protection statement or privacy policy***

	made available to the data subject at the time of obtaining his or her consent.

Justification

The draft Regulation should provide common and practical examples of how processing activities can be communicated to individuals for the purposes of obtaining consent for a range of activities in a single step. It should also allow controllers to define the most appropriate channel and level of information to be provided to data subjects for each processing activity. The information to be provided for the purposes of obtaining the data subject's consent shall be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles (considered below in the justification for the proposed changes to Article 4(8)).

Recital 34 (EC proposal)	Recital 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.	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. ***However, a data controller may legitimately make consent to the processing a condition of access to a service, particularly when the service is free of charge to the data subject.*** 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.

Justification

Controllers should be able to make consent to the processing a condition of access to a

service which may not be otherwise free. See also the proposed changes to Article 7(4).

Article 4(8) (EC proposal)	Article 4(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;	'the data subject's consent' means any freely given specific, informed and ~~*explicit*~~ ***unambiguous*** indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action ***or by any other method***, signifies agreement to personal data relating to them being processed. ***The information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with Article 5;***
Justification Unambiguous consent should be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (…) when the actions lead to an unmistakable conclusion that consent is given". The highly prescriptive nature of the requirements for consent could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk of inundating users with tick boxes and warnings. As well as affecting the user experience, this inevitably will lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it. The controller is in the best position to decide the appropriate level of information to provide individuals about specific processing activities. The information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles under Article 5.	

Article 7 (EC proposal)	Article 7
1. The controller shall bear the burden of	1. ***For the purposes of Article 9(2)(a), t***he

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. 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.	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. ***The data subject's consent may be exercised by a single step provided that all relevant matters to which the consent relates are made clearly available.*** 3. The data subject shall have the right to withdraw his or her consent at any time ***and the data controller shall be entitled to suspend or terminate the provision of services to the data subject where such provision relies on the consent to the processing withdrawn by the data subject.*** 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, ***except where consent to the processing may legitimately constitute a condition of access to a service by the data subject.***
Justification The controller should only bear the 'burden of proof' in cases where the need for consent is in connection with the processing of sensitive personal data. Controllers should be entitled to obtain consent for a range of data processing activity in a single step as long as they provide them the appropriate level of information for each processing activity. Controllers should not be obliged to continue to offer services where individuals decline to provide their personal data. The controller shall be entitled to suspend or terminate	

services where such provision of services relies on consent to the processing which has been withdrawn by the individual.

Controllers should also be able to make consent to the processing a condition of access to a service which may not be otherwise free.

3. Right to be forgotten

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, the right to be forgotten needs very careful consideration. As drafted, apart from not harmonising national laws, it raises major concerns with regard to the right of others to remember and of freedom of expression. There is also a risk that it could result in measures which are technically impossible to apply in practice and therefore make for bad law. A right balance should be found between data subject's right to get their data deleted, the fundamental rights of other individuals and the reality of the online environment. The proposal prescribes a right for people to have their data deleted and also requires data controllers to take all reasonable steps to obtain erasure of content copied to a third party website or application.

It is important to differentiate between three challenges presented by the 'right to be forgotten':

The *first* is in relation to people who have posted personal information about themselves online and later wish to delete that information.

The *second* is in relation to the practical difficulty to identify the necessary information to ensure compliance with the right to be forgotten. This challenge arises in two specific situations:

- The first situation concerns the deletion of personal data of an individual made available online by another individual. In practice, the operator of a website or hosting platform is unlikely to know in many cases which information available on the platform constitutes the personal data that should be deleted. It is virtually impossible to control what information millions of users may make available about other individuals – many of whom will not be users themselves – and to determine where all of the information is and whether that information is the personal data of the person making the request. Therefore a broad obligation to delete any information made available by users upon request of other individuals would be likely to present major implementation challenges to the extent that it would be practically unworkable.

- The second situation concerns the specific provision under Article 17(2), which requires informing third parties of the request for deletion of links to or copies of

an individual's personal data. This would involve identifying any such links or copies of the information elsewhere on the Internet and communicating with those responsible for placing the links or copying the information to request such links or information to be deleted. Again, we do not see any practicable means for services like social networking to control which links to or copies of someone's personal data exist in other places on the Internet, let alone communicate with the third parties responsible for their dissemination.

In order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the Internet. There is concern in the Internet community that 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.

The *third* is in relation to any personal data made publicly available and the fact that there may be strong grounds to justify under certain circumstances the right of others to know certain facts concerning individuals, as this is closely linked to the right to freedom of expression and other democratic values. It is clear that there is a potential conflict between the right for people to express themselves and the privacy rights of others. It is important to consider fully the implications on the open Internet and personal expression as we determine the right balance. The scope of freedom of expression contained in Article 80 and further clarified in Recital 121 is defined quite narrowly and should be extended to cover for example mere expressions of opinion, user generated content and more generally recognise the nature of new forms of communication such as blogging and social networking.

Finally, the debate on the "right to be forgotten" affects a number of Internet services, which rely on user-generated content. This issue is not unique to social networking. Policy makers should take into account the "right of others to remember" and reach a balanced conclusion which respects freedom of expression.

<u>Drafting recommendations</u>:

Recital 53 / Article 17 (Right to be forgotten and to erasure): The right to erasure in Article 17(1) is welcome, but the wording should be amended to ensure that it balances the competing interests set out above As such, we propose that:

- Where a third party makes information about another individual available online, it is not always possible for a controller to identify all of the related personal data. Therefore we have suggested that the right of an individual to require erasure when it is 'impossible or involves a disproportionate effort' (Article 17(1)(e)).

- The right of erasure may be overridden by the interests or fundamental rights and freedoms of others (Article 17(1)(f) and Recital 53).

- The right to be forgotten, as drafted, raises major concerns with regard both to the right of others to remember and to freedom of expression. Moreover, 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. We therefore resist the wording contained in Article 17(2) and Recital 54.

- An exemption should apply when a controller wishes to process the information for a certain legitimate purpose (such as the provision of system, network or information security). This position should be limited to circumstances where the interests of the controller are not outweighed by those of the individual and we have therefore proposed changes to Recital 53 in this regard.

Drafting suggestions:

Recital 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. 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	Recital 53 Any person should have the right to have personal data concerning them rectified 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. ~~*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, ***certain exemptions should apply, particularly when***

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.	***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 legitimate interest, as for instance for the purpose of providing system, network or information security.*** ~~*and*~~ ***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:

- Where a third party makes information about another individual available online, it is not always possible for a controller to identify all of the related personal data;
- Where an individual makes information their information publicly available, there is a potential conflict between the right of others to know and the right of others to remember (including where the data subject has given their consent as a child);
- The right to know is closely linked to the right to freedom of expression and other democratic values; and
- An exemption to the right to be forgotten should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security.

Recital 54 To strengthen the right to ***erasure*** in the online environment, ***such*** right should also be extended in such a way that a	***delete***

controller who has ***transferred*** the personal data ***or made them*** public ***without being instructed to do so by the data subject*** 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.	

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.

Article 6 (EC proposal)	Article 6
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	(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; (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; (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. 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: (a) Union law, or (b) the law of the Member State to which the controller is subject. 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	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; (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; (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. ***The processing of data to the extent necessary for the purpose of providing system, network or information security constitutes a legitimate interest of the data controller.*** 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: (a) Union law, or (b) ***a legally binding obligation*** to

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 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.	which ***a*** controller is subject. The ***legally binding obligation*** 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 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.
Justification An exemption to the right to be forgotten should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security.	

Article 13(1) Any rectification or erasure carried out in accordance with Articles 16 and 17 ***is extended*** to each recipient to whom the data have been disclosed ***without the control of the data subject***.	Article 13(1) Any rectification or erasure carried out in accordance with Articles 16 and 17 ***is extended*** to each recipient to whom the data have been disclosed ***without the control of the data subject***, ***unless this proves impossible or involves a disproportionate effort***.
Justification Retain the European Commission's proposal to the extent that this obligation should not apply where compliance would be impossible or involve a disproportionate effort in addition to the language proposed by the rapporteur.	

Article 17 – Right to ***erasure***	Article 17 – Right to erasure
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, ~~*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:
(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 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;	(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 processing of the data;
(c) the data subject objects to the processing of personal data pursuant to Article 19;	(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.	(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.
2. Where the controller referred to in paragraph 1 has ***transferred*** the personal data***, or has made such data*** public ***without being clearly instructed by the data subject to do so***, 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	~~*2. Where the controller referred to in paragraph 1 has transferred the personal data, or has made such data public without being clearly instructed by the data subject to do so, 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,*~~

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. 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; (e) in the cases referred to in paragraph 4. 4. Instead of erasure, the controller shall restrict processing of personal data where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; (d) the data subject requests to transmit	~~*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.*~~ 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; (e) in the cases referred to in paragraph 4. 4. Instead of erasure, the controller shall restrict processing of personal data where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; (d) the data subject requests to transmit the personal data into another automated

the personal data into another automated processing system in accordance with Article 18(2). 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest. 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing. 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. 8. Where the erasure is carried out, the controller shall not otherwise process such personal data. 9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying: (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	processing system in accordance with Article 18(2). 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest. 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing. 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. 8. Where the erasure is carried out, the controller shall not otherwise process such personal data. ~~*9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:*~~ ~~*(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;*~~ ~~*(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;*~~ ~~*(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.*~~
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. The right to erasure in Article 17(1) 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;
- An exemption should apply when a controller wishes 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.

For the reasons above and because the right to erasure is sufficient to give data subjects control over their personal data, Article 17(2) should be deleted.

4. Profiling

The specific provisions on "profiling" contained in the draft Regulation are unnecessary, over-broad, and legally vague. Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.

Article 20 extends the scope of the 95/46/EC Directive provisions relating to automated individual decisions to cover a range of new factors including location, personal preferences and behaviour. It also introduces a new and undefined test of "significant effect". Failure to adequately distinguish between processing with legal or significant effect and content customization could indiscriminately subject a potentially enormous range of activity (and yet-to-be-invented applications) across every industry sector to the stricter consent provisions of Article 7 and the provisions relating to prior authorization as defined in Article 33 and 34. As well as being burdensome on data protection authorities, this fails to strike an appropriate balance between protecting the rights of individuals and safeguarding innovation and commerce. Customization is an essential element in a competitive online marketplace, and such broadly-framed provisions are likely to have unintended consequences and affect many legitimate practices in the process negatively.

Measures on profiling do not distinguish between the technology and its use. The current drafting of the Regulation shows that there is no recognition of positive uses of profiling and no differentiation is made between the technology and its uses. Article 20 clearly violates the principle of technology neutrality which is alluded to in Recital 13, and which is critically important in crafting future-proof regulation. Given the numerous other safeguards in this draft Regulation, profiling techniques do not need be treated differently to any other type of personal data processing.

The legitimate interests of the data controller should provide a legal basis for "profiling". The legitimate interests pursued by a controller should be an additional legal ground for lawful profiling, along with consent, in order to ensure that profiling techniques and technologies that do not aim at identifying data subjects but at extracting aggregate baseline data that can be used to manage, improve or customize services for similar customers are not prohibited under the draft Regulation. It is important that this be the case here as with other sections of the draft Regulation, to ensure that the use of profiling techniques for legitimate purposes such as security, anti-fraud, accounting are not prohibited**.**

<u>Drafting recommendations</u>:

Recital 51 / Recital 58 / Recital 59 / Article 20 (Measures based on Profiling): Prohibiting or severely restricting profiling is not adequate for a technique that is enabled by various technologies, is used across sectors for various purposes and, whilst potentially presenting risks in certain cases, also has benefits for consumers, business and the economy.

Recital 13 recognises that, in order to avoid a serious risk of circumvention, "the protection of individuals should be technologically neutral and not depend on the techniques used". Article 20 clearly violates this principle of technology neutrality, which should be core to any laws that deal with technology if they are to withstand the test of time and technology evolution.

Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.

Therefore, it is proposed that Recital 51, Recital 58 and Article 20 be entirely deleted, as well as a reference in Recital 59.

Drafting suggestions:

Recital 51 (EC proposal) 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.	***delete***
Justification Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole. Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.	

Recital 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 ***forbidden only*** when expressly ***stated*** by law, ***not*** carried out in the course of entering or performance of a contract, or when the data subject has ***withdrawn*** 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. ***The data subject, when this profiling is not necessary for entering or performing a contract, should always have the possibility to opt-out.***	***delete***
Justification Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole. Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.	

Recital 59 (EC proposal) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of	Recital 59 Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, ~~*measures based on profiling,*~~ as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of

human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.
Justification Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole. Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.	

Article 20 ~~*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.*~~	***delete***

2. Subject to the other provisions of this Regulation, a ***measure which produces legal effects on a*** person ***or significantly affects this person, based solely on automated processing intended to evaluate certain personal aspects relating to this person or to analyse or predict in particular the person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour, is lawful*** only if the processing: (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) expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 ***in Article 15 and Article 16***. 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. 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

Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size -fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.
Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.

5. Controller/Processor

The concepts of data processor and data controller have been appropriately defined in the existing data protection legislation (i.e. Directive 95/46/EC). In the draft Regulation, the concept of data processor is not clearly defined and, as a result, there may be situations where a data processor may unjustifiably be regarded as a data controller. For example, under Article 26(4), if a processor is considered to be taking independent decisions then that processor will be deemed as a controller. In practice, the interaction between the two concepts might raise practical difficulties when a data controller and a data processor are part of the same company group and both parts of the group collaborate on a daily basis. The policies and protocols will be defined by the data controller, but often implemented independently by the data processor.

Drafting recommendations:

Recital 62 / Article 4(5) (Definition of Controller) / Article 4(6) (Definition of Processor) / Article 24 (Joint Controllers) / Article 26 (Processor): Proposals regarding the definition of the data controller need to be narrowed down to ensure that organisations can operate efficiently with legal certainty. The definition of data processor should also be modified to allow certain elements of co-decision-making.

Article 22 (Responsibility of the Controller): This provision introduces new accountability provisions on controllers. These include requirements to demonstrate compliance with the draft Regulation through the adoption of internal policies, assignment of internal responsibilities and verification of compliance. Even though these provisions are sound, there may be some difficulty in situations where the level of prescription in the draft Regulation is such that they may not reflect practices that are otherwise appropriate to safeguard personal data. To this end the Article would requires further consideration.

Recital 65 / Article 28 (Documentation) / Article 9 (Co-operation with the supervisory authority): Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers are unduly burdensome. We have therefore suggested that the obligations placed on controllers as regards documentation (Article 28(1), (3) and (4)) and co-operation with the competent supervisory authority (Article 29(1)) should not extend to processors.

Drafting suggestions:

Recital 62 (EC proposal)	Recital 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 behalf of a controller.	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 behalf of a controller.
Justification The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).	

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

Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers are unduly burdensome.

Article 4(5) (EC proposal)	Article 4(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;	'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;
Justification The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).	

Article 4(6) (EC proposal)	Article 4(6)
'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	'processor' means a natural or legal person, public authority, agency or any other body which processes personal data, ***including making decisions with regard to the processing*****,** on behalf of the controller;
Justification The definition of processor as it is worded in the draft Regulation does not reflect current practices. It would be consistent with current practices to allow processors to undertake certain decision making responsibilities without losing their processor status, as long as such processing continues to take place on behalf of a controller.	

Article 15(d)	Article 15(d)
the period for which the personal data will be stored ***and the time of collection***;	the period for which the personal data will be stored ~~*and the time of collection*~~~~;~~

Justification Retain the European Commission's proposal. The obligation added by the rapporteur has the potential of being administratively burdensome for the controller.

Article 22 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.	Article 22 The controller shall adopt policies and implement appropriate ***and reasonable*** measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. ***For the purpose of this Regulation, appropriate and reasonable measures will mean measures that are proportional to the risks involved, the administrative burdens and costs of the implementation, and the state of and availability of the technology.***
2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1).	2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the ***competent*** supervisory authority pursuant to Article 34(1) and (2); (e) 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.	3. The controller shall implement mechanisms ~~*to ensure*~~ ***for*** 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.
Justification	

The obligations on controllers to adopt policies and appropriate measures should be clear. Such policies and measures should be "appropriate and reasonable" and proportional to the "risks involved, the administrative burdens and costs of the implementation, and the state of and availability of the technology".

Article 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. ***Where such determination is lacking or is not sufficiently clear, the data subject can exercise his rights with any of the controllers and they shall be equally liable.***	Article 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.
Justification The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).	

Article 26 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	Article 26 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; (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.	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; (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;*~~ ***not conflict with the instructions given by the controller when enlisting another processor;*** (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*~~ ***29*** to 34; (g) ~~*hand over all results to the controller after the end of the processing and not process the personal data otherwise;*~~ ***not process the personal data further after the end of the agreed processing;*** (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.	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.

Justification

The definition of processor as it is worded in the draft Regulation does not reflect current practices. It would be consistent with current practices to allow processors to undertake certain decision making responsibilities without losing their processor status, as long as such processing continues to take place on behalf of a controller. In particular:

Processors should be able to enlist sub-processors that enable the requirements of the Regulation to be met (rather than only with the prior permission of the controller (Article 26(2)(d)).

Processors should not be able to process personal data after the end of the agreed processing (rather than being required to hand over all results to the controller after the end of the processing and not process the personal data otherwise (Article 26(2)(g).

Processors should provide information to the controller necessary to control compliance with the obligations laid down in the Article but not to the supervisory authority (Article 26(2)(h)).

Article 28 1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility. 2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (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); (d) a description of categories of data	Article 28 1. Each controller ~~*and processor*~~ and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility. 2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (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); (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 ***and, in an electronic format, to the data subject***. 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 that is processing personal data only as an activity ancillary to its main activities. 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).	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 ***competent*** 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. 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).
Justification Processors should not be subject to the same administrative obligations as controllers. The administrative processor related obligations to keep the same documentation as	

controllers is unduly burdensome. The obligations placed on controllers as regards documentation (Article 28(1), (3) and (4)) should not extend to processors. References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions (Article 51).

Article 29 (EC proposal) 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. 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.	Article 29 1. The controller ~~*and the processor*~~ and, if any, the representative of the controller, shall co-operate, on request, with the ***competent*** 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 ***competent*** 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 ***competent*** supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the ***competent*** supervisory authority.
Justification References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions (Article 51). Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers is unduly burdensome. Therefore the obligations placed on controllers as regards co-operation with the competent supervisory authority (Article 29(1)) should not extend to processors.	

International Transfers

Article 41(2)(a)	Article 41(2)(a)

the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, ***jurisprudential precedents*** as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;	the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, ~~*jurisprudential precedents*~~ as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;
Justification The European Commission should not be granted the power to give consideration to judicial precedents. This would be most appropriately dealt with by the European Court of Justice whose primary function is to interpret the law, rather than the Commission.	