ADDENDUM to Opinion 3/2015

RECITALS

This four-column table presents three versions of the GDPR in their original formatting together with the EDPS recommendations.

- Column 1: the Commission proposal contains no special formatting;
- Column 2: the 1st reading position of the European Parliament: text additional to the Commission proposal is marked in bold italics; text deleted from the Commission proposal is struck through; where a paragraph or article is wholly identical with the Commission proposal, the cell is marked with a diagonal line;
- Column 3: the General Approach of the Council: text additional to the Commission proposal is marked in bold italics; text deleted from the Commission proposal is struck through; text from the Commission proposal which has been moved up or down is marked in bold;
- Column 4: EDPS recommendations. No special formatting. The numbering of the three texts remains unchanged. In most cases, the recommendation contains amended or unchanged text. In other instances, paragraphs or articles found in the other texts may have been deleted, merged or moved.

COM(2012)0011	EP Position / First Reading	Council General Approach (15/06/2015)	EDPS recommendations
Whereas:	Whereas:	Whereas:	Whereas:
(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.	(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ('Charter') and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.	(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.	(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.
(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the	(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the	(2) The ~~processing of personal data is designed to serve man; the~~ principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the	(2) The processing of personal data should be designed to serve man. Whatever the nationality or residence of natural persons, it should respect their human dignity as well as their fundamental rights and freedoms, notably their right to the protection of personal data and contribute to the well-being of individuals, to economic and social progress, to the accomplishment of an area of freedom, security and justice, and to trade expansion.

strengthening and the convergence of the economies within the internal market, and the well-being of individuals.	strengthening and the convergence of the economies within the internal market, and the well-being of individuals.	strengthening and the convergence of the economies within the internal market, and the well-being of individuals.	

(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.	(3) Directive 95/46/EC of the European Parliament and of the Council[1] ~~of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data~~[2] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States. ***1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).***	(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.	(3) Directive 95/46/EC* seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States. _____ **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).*
		(3a) ***The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality. This Regulation***	

[1] OJ L 281, 23.11.1995, p. 31.
~~[2] OJ L 281, 23.11.1995, p. 31.~~
[3] OJ L 281, 23.11.1995, p. 31.

		***respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity*.**	

(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.	(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.	(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between ~~economic and social,~~ public and private actors**,** ***including individuals and undertakings*** across the Union ***has*** increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.	

(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.	(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.	(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and ~~requires to~~ ***should*** further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.	(5) Rapid technological developments, globalisation and the rise of the digital economy have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Technology has transformed both the economy and social life, and the legal framework for personal data protection should be updated and modernised accordingly.

(6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.	(6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.	(6) These developments require ~~building~~ a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance ~~to~~ **of** ~~create~~ **creating** the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.	(6) These developments require a stronger and more coherent data protection framework in the Union, providing legal and practical certainty for economic operators, public authorities and individuals who should be in control of their own data, backed by strong enforcement.
		(6a) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for the coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of the Regulation in their respective national law.	

(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.	(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.	(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.	(7) While the objectives and principles of Directive 95/46/EC remain sound, it has been implemented and applied differently across the Union, resulting in legal uncertainty, creating obstacles to the pursuit of economic activities at the level of the Union and distorting competition. The adoption of a Regulation should ensure consistent and homogenous application of data protection rules throughout the Union, thus eliminating divergences hampering the free movement of data within the internal market.

(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.	(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.	(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data ***within the Union***, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. ***Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC Member States have several sector specific laws in areas that need more specific***	(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.

		provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules. Within this margin of manoeuvre sector-specific laws that Member States have issued implementing Directive 95/46/EC should be able to be upheld.	
			(8a) Several provisions of this Regulation either build on national law or allow or require national law to give effect to, further specify, or depart from its provisions under certain conditions. Such national laws must be adopted (or amended if they are not compatible with this Regulation). National laws should be aligned with the provisions of this Regulation, including the general principle of free movement of personal data within the Union. Within the limits of this Regulation, the law of the Member States may provide details to ensure the lawfulness and fairness of processing.
(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the	(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the	(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the	(9) Effective protection of personal data throughout the Union requires harmonised powers for monitoring and ensuring compliance, as well as

obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.	obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.	obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.	equivalent dissuasive sanctions for offenders across the Member States.
(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.	(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.	(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data	(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this	(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this	(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. ***The proper functioning of the internal market requires that the free movement of personal data within the Union should not be restricted or prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.*** To take account of the specific	(11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this

Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.	Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC[1] ~~of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises~~. [1] ***Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).***	situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.	Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. The proper functioning of the internal market requires that the free movement of personal data within the Union should not be restricted or prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.	(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.	(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. ~~This should also apply where the name of the legal person contains the names of one or more natural persons.~~	(12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons, and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person.

(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.	(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.	(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.	(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.

	Amendment 1		
(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001[4], or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.	(14) This Regulation does not This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law~~, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to~~**.** Regulation (EC) No 45/2001~~, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union~~ ***of the European Parliament and of the Council[1] should be brought in line with this Regulation and applied in accordance with this Regulation***. _____ ***[1] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of***	(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, ***such as activities concerning national security,*** nor does it cover the processing of personal data by the ~~Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001[5], or the processing of personal data by the~~ Member States when carrying out activities in relation to the common foreign and security policy of the Union.	(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies which are subject to Regulation (EC) No 45/2001*, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union. _____ ** Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).*

[4] ***OJ L 8, 12.1.2001, p. 1.***

[5] ~~OJ L 8, 12.1.2001, p. 1.~~

	personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1***)***.		
		(14a) Regulation (EC) No 45/2001 applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001[6] and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation.	(14a) Regulation (EC) No 45/2001 applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of this Regulation.

6 ***OJ L 8, 12.1.2001, p. 1.***

	Amendment 2		
(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. The exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.	(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal***, family-related,*** or domestic, such as correspondence and the holding of addresses ***or a private sale***~~,~~ and ~~without any gainful interest and thus~~ without any connection with a professional or commercial activity. ~~The exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.~~ ***However, this Regulation should apply to controllers and processors which provide the means for processing personal data for such personal or domestic activities.***	(15) This Regulation should not apply to processing of personal data by a natural person ***in the course of a***~~, which are exclusively~~ personal or ~~domestic~~***household activity***~~, such as correspondence and the holding of addresses, and without any gainful interest~~ and thus without ~~any~~ **a** connection with a professional or commercial activity. ***Personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities. However, this Regulation*** ~~The exemption~~ should ~~also not~~ apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.	(15) This Regulation should not apply to processing of personal data by a natural person in the course of an exclusively personal or household activity and thus without a connection with a professional or commercial activity. Personal and household activities normally include social networking. However, this Regulation should apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.
(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of	(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of	(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences ~~or~~ the execution of criminal penalties ***or the safeguarding***	(16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of

such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY).	such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive ~~XX/YYY~~***(Directive 2014/.../EU of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data***).	***against and the prevention of threats to public security***, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY). ***Member States may entrust competent authorities within the meaning of Directive XX/YYY with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, fallw***	such data, is the subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive 2014/.../EU of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and the free movement of such data).

		within the scope of this Regulation. ***With regard to the processing of personal data by those competent authorities for purposes falling within scope of the General Data Protection Regulation, Member States may maintain or introduce more specific provisions to adapt the application of the rules of the General Data Protection Regulation. Such provisions may determine more precisely specific requirements for processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State.*** ***When processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard***	

		specific important interests including public security and the prevention, investigation, detection and prosecution of criminal offences. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.	

		(16a) **While this Regulation applies also to the activities of courts** ***and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities.*** **The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity,** ***in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including its decision-making. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular*** **control compliance with the rules** ***of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.***	

(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC ***of the European Parliament and of the Council***[1], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. [1] ***Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1).***	(17) ***Directive 2000/31/EC does not apply to questions relating to information society services covered by this Regulation. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States. Its application should not be affected by this Regulation.*** This Regulation should ***therefore*** be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council*, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. _____ ** Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1).*

	Amendment 3		
(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation.	(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. ***Personal data in documents held by a public authority or public body may be disclosed by that authority or body in accordance with Union or Member State law regarding public access to official documents, which reconciles the right to data protection with the right of public access to official documents and constitutes a fair balance of the various interests involved***.	***(18) deleted***	(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation.

(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.	(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.	(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.	(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

	Amendment 4		
(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.	(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects ~~residing~~ in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services***, irrespective of whether connected to a payment or not,*** to such data subjects, or to the monitoring ~~of the behaviour~~ of such data subjects. ***In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects in one or more Member States in the Union.***	(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects~~, or to the monitoring of the behaviour of such data subjects~~ ***irrespective of whether connected to a payment or not, which takes place in the Union. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language***	(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of such data subjects, irrespective of whether connected to a payment or not.

		generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union.	

	Amendment 5		
(21) In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	(21) In order to determine whether a processing activity can be considered to 'monitor ~~the behaviour~~' ~~of~~ data subjects, it should be ascertained whether individuals are tracked ~~on the internet with~~***, regardless of the origins of the data, or if other data about them are collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of*** data processing techniques which consist of applying a 'profile' ~~to an individual~~, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	(21) ***The processing of personal data of data subjects residing in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of their behaviour taking place within the European Union.*** In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of ~~applying a 'profile' to~~ ***profiling*** an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	(21) The processing of personal data of data subjects in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of such data subjects. In order to determine whether a processing activity can be considered as such monitoring, it should be ascertained whether individuals are tracked, regardless of the origins of the data, or if other data about them are collected, for example from public sources, including the potential use of data processing techniques such as profiling.

(22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.	(22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.	(22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.	(22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.
	Amendment 6		
(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	(23) The principles of **data** protection should apply to any information concerning an identified or identifiable **natural** person. To determine whether a person is identifiable, account should be taken of all the means ~~likely~~ reasonably **likely** to be used either by the controller or by any other person to identify **or single out** the individual **directly or indirectly**. **To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological**	(23) The principles of ***data*** protection should apply to any information concerning an identified or identifiable ***natural*** person. ***Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person.*** To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual ***directly or indirectly***. ***To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective***	(23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information relating to an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify or single out the individual, directly or indirectly. To ascertain what means are reasonably likely to be used to identify the individual, account

	development. The principles of data protection should **therefore** not apply to **anonymous** data ~~rendered anonymous in such a way that the data subject is no longer identifiable~~**, which is information that does not relate to an identified or identifiable natural person**. **This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes**.	***factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.*** The principles of data protection should ***therefore*** not apply to ***anonymous information, that is information which does not relate to an identified or identifiable natural person or to*** data rendered anonymous in such a way that the data subject is ***not or*** no longer identifiable. ***This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes.***	should be taken of all objective factors, such as the cost, the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and scientific purposes.
		(23aa) The principles of data protection should not apply to data of deceased persons. The national law of a Member State may provide for rules regarding the processing of data of deceased persons.	

		(23a) The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of 'pseudonymisation' through the articles of this Regulation is thus not intended to preclude any other measures of data protection. ***23b) (…)***	
		(23c) In order to create incentives for applying pseudonymisation when processing personal data, measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure that the provisions of this Regulation are implemented, taking into account the respective data processing and ensuring that additional information for	

		attributing the personal data to a specific data subject is kept separately. The controller who processes the data shall also refer to authorised persons within the same controller. In such case however the controller shall make sure that the individual(s) performing the pseudonymisation are not referenced in the meta-data.	
	Amendment 7		
(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.	(24) ~~When using online services, individuals may be associated with online~~ ***This Regulation should be applicable to processing involving*** identifiers provided by ~~their~~ devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers ***and Radio Frequency Identification tags, unless those identifiers do not relate to an identified or identifiable natural person***. ~~This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers,~~	(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, ***when*** combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. ~~It follows that i~~**I**dentification numbers, location data, online identifiers or other specific factors as such ~~need~~ ***should*** not ~~necessarily~~ be considered as personal data~~in all circumstances~~ ***if they do not identify an individual***	(24) This Regulation should apply to processing involving identifiers provided by devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers and Radio Frequency Identification tags, unless those identifiers do not relate to an identified or identifiable natural person.

	~~location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances~~.	***or make an individual identifiable.***	
	Amendment 8		
(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	(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 ***that is the result of choice*** by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data~~, including by~~***. Clear affirmative action could include*** 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 his or her personal data. Silence***, mere use of a service*** 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	(25) Consent should be given ~~explicitly~~ ***unambiguously*** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a ***written, including electronic, oral*** ~~***or other***~~ statement or***, if required by specific circumstances,*** by ***any other*** clear affirmative action by the data subject, ***signifying his or her agreement to*** ~~ensuring that individuals are aware that they give their consent to the processing of~~personal data ***relating to him or her being processed.***~~,~~ ***This could*** ~~including~~ **include** ~~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. ***Where it is technically feasible and***	(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, signifying his or her agreement to personal data relating to him or her being processed. Clear affirmative action could include ticking a box when visiting an Internet website or any other statement or conduct, which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application. Silence, mere use of a service or inactivity should therefore not constitute consent. Consent should

disruptive to the use of the service for which it is provided.	request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	***effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application***. ***In such cases it is sufficient that the data subject receives the information needed to give freely specific and informed consent when starting to use the service.*** Consent should cover all processing activities carried out for the same purpose or purposes. ***When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes.*** If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	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 and concise and not disruptive to the use of the service for which it is provided.

		(25a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.	
		(25aa) It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection. Therefore data subjects can give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose and provided that this does not involve disproportionate efforts in view of the protective purpose.	

(26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	(26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	(26) Personal data ~~relating to~~ ***concerning*** health should include ~~in particular all~~ data pertaining to the health status of a data subject ***which reveal information relating to the past, current or future physical or mental health of the data subject***; ***including*** information about the registration of the individual for the provision of health services; ~~information about payments or eligibility for healthcare with respect to the individual;~~ a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; ~~any information about the individual collected in the course of the provision of health services to the individual;~~ information derived from the testing or examination of a body part or bodily substance, including ***genetic data and*** biological samples; ~~identification of a person as provider of healthcare to the individual;~~ or any information on ~~e.g.~~ ***for example*** a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as	(26) Personal data concerning health should include in particular all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject; including information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as

		~~e.g.~~ ***for example*** from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	e.g. from a physician or other health professional, a hospital, a medical or other device, or an in vitro diagnostic test.
(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.	(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, ~~conditions~~ and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.	(27) The main establishment of a controller in the Union should be ***the place of its central administration in the Union, unless*** ~~determined according to objective criteria and should imply the effective and real exercise of management activities determining~~ the ~~main~~ decisions ~~as to~~ ***on*** the purposes~~, conditions~~ and means of processing ***of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment.*** ~~through stable arrangements.~~ ***The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements.*** This criterion should not depend ***on*** whether the processing of personal data is	(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. This criterion should not depend on 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 not determining criteria for a main establishment.

		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***t*** determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union ***and, if it has no central administration in the Union, the place where the main processing activities take place in the Union***. ***In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment but the supervisory authority of the processor should be considered as a concerned supervisory authority and participate to the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be***	

		considered as concerned supervisory authorities when the draft decision concerns only the controller. ***Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.***	

(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. ***A central undertaking which controls the processing of personal data in undertakings affiliated to it forms together with these undertakings an entity which may be treated as "group of undertakings".***	(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.

	Amendment 9		
(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. ~~To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.~~ ***Where data processing is based on the data subject's consent in relation to the offering of goods or services directly to a child, consent should be given or authorised by the child's parent or legal guardian in cases where the child is below the age of 13. Age-appropriate language should be used where the intended audience is children. Other grounds of lawful processing such as grounds of public interest should remain applicable, such as for processing in the context of preventive or counselling services offered directly to a child.***	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. ~~To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.~~ ***This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child.***	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.
(30) Any processing of personal data should be lawful, fair and	(30) Any processing of personal data should be lawful, fair and	(30) Any processing of personal data should be lawful ***and***~~,~~ fair***.*** ~~and~~	(30) Any processing of personal data should be lawful, fair and

transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.	transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.	***It should be*** transparent ~~in relation to~~ ***for*** the individuals ~~concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means.~~ ***that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and***	transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if and as long as the purpose of the processing could not be fulfilled by other means, in particular by processing information that does not involve personal data. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the conttroller for erasure or for a periodic review.

		the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them. ***Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate and relevant for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than***	

		necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. ~~In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.~~ ***Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or the use of personal data and the equipment used for the processing.***	

	Amendment 10		
(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.	(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation. ***In case of a child or a person lacking legal capacity, relevant Union or Member State law should determine the conditions under which consent is given or authorised by that person.***	(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation***, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity 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***.	(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.

		(31a) Wherever this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant the constitutional order of the Member State concerned, however such legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union and the European Court of Human Rights.	

	Amendment 11		
(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.	(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. ***To comply with the principle of data minimisation, the burden of proof should not be understood as requiring the positive identification of data subjects unless necessary. Similar to civil law terms (e.g. Council Directive 93/13/EEC[1]), data protection policies should be as clear and transparent as possible. They should not contain hidden or disadvantageous clauses. Consent cannot be given for the processing of personal data of third persons.*** ***[1] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).***	(32) Where processing is based on the data subject's consent, the controller should ~~have the burden of proving~~ ***be able to demonstrate*** 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~~ ***the*** extent ***to which*** consent is given. ***A declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and its content should not be unusual within the overall context. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment.***	(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.

	Amendment 12		
(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.	(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment. ***This is especially the case if the controller is a public authority that can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given. The use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes, does not express free consent. Consent for the processing of additional personal data that are not necessary for the provision of a service should not be required for using the service. When consent is withdrawn, this may allow the***	***(33) deleted***	

	termination or non-execution of a service which is dependent on the data. Where the conclusion of the intended purpose is unclear, the controller should in regular intervals provide the data subject with information about the processing and request a re-affirmation of ~~their~~ his or her consent.		
	Amendment 13		
(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	***deleted***	(34) ***In order to safeguard that*** ~~Consent~~ **consent** ***has been freely-given, consent*** should not provide a valid legal ground for the processing of personal data ***in a specific case,*** ~~,~~ where there is a clear imbalance between the data subject and the controller ***and*** ~~This~~ **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~~	(34) When assessing whether consent is freely given, it must be considered, among others, whether there is a significant imbalance between the data subject and the controller. This may be the case, for example, where the data subject is in a situation of dependence from the controller, such as in the employment context or where the controller is a public authority. Consent is presumed not to be freely given if it does not allow separate consent to be given to different data processing operations even though it is appropriate in the individual case, or if the performance of a contract is made dependent on the consent even

deemed as freely given, taking into account the interest of the data subject.		~~authority can impose an obligation by virtue of its relevant public powers and~~ ***makes it unlikely that*** ~~the~~ consent ~~cannot be deemed~~ ***was given*** ~~as~~ freely~~- given, taking into account the interest of the data subject~~ ***in all the circumstances of that specific situation. Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it is appropriate in the individual case, or if the performance of a contract is made dependent on the consent despite this is not necessary for such performance and the data subject cannot reasonably obtain equivalent services from another source without consent.***	though this is not necessary for such performance and the data subject cannot reasonably obtain equivalent services from another source without consent.
(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.	(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.	(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.	(35) Processing should be lawful where it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

		(35a) This Regulation provides for general rules on data protection and that in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data.	

	Amendment 14		
(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.	(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. ***This should include also collective agreements that could be recognised under national law as having general validity.*** It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.	(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a ~~legal~~ basis in Union law, or in ***the national law of*** a Member State ~~law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms~~. It ~~is~~ ***should be*** also for Union or national law to determine ***the purpose of processing.*** ~~whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association~~. ***Furthermore, this basis could specify the general conditions of the Regulation governing the lawfulness of data processing, determine***	(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law, such as a professional association. Within the limits of this Regulation the law of the Member State may provide details to ensure the lawfulness and fairness of processing. The notion of processing necessary for the performance of a task carried out in

		specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.	the public interest includes the processing of personal data necessary for the management and functioning of public authorities.

(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.	(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.	(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life ***or that of another person***. ***Some types of data processing may serve both important grounds of public interest and the vital interests of the data subject as, for instance when processing is necessary for humanitarian purposes, including for monitoring epidemic and its spread or in situations of humanitarian emergencies, in particular in situations of natural disasters.***	(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life or that of another person.

	Amendment 15		
(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	(38) The legitimate interests of ~~a~~ ***the*** controller***, or in case of disclosure, of the third party to whom the data ~~is~~ are disclosed,*** may provide a legal basis for processing, provided ***that they meet the reasonable expectations of the data subject based on his or her relationship with the controller and*** that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. ***Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, processing limited to pseudonymous data should be presumed to meet the reasonable expectations of the data subject based on his or her relationship with the controller.*** The data subject should have the right to object the processing~~, on grounds relating to their particular situation and~~ free of charge. To ensure transparency, the controller should	(38) The legitimate interests of a controller ***including of a controller to which the data may be disclosed or of a third party*** may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. ~~This would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place.~~ ***Legitimate interest could exist for example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place.*** ~~i~~**I**n particular ~~where~~ ***such assessment must take into***	(38) The legitimate interests of the controller, or by the third party or parties to whom the data are disclosed, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks. The interests and fundamental rights of the data subject could in particular override the interest of the controller where personal data are processed in circumstances where

	be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. ***The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.*** Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	***account whether*** the data subject is a child, given that children deserve specific protection. The data subject should have the right to object ***to*** the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. ~~Given that it is for ***Union or national law*** the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the ***exercise*** performance of their tasks***duties***.~~	data subjects do not reasonably expect processing. When assessing whether the interests and fundamental rights of the data subject could override the interest of the controller, account should be taken in particular of: (a) the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their use; (b) the nature of the personal data and the impact of the processing on the data subjects; and (c) the safeguards applied to ensure fair processing and to prevent any undue impact on data subjects.

		(38a) Controllers that are part of a group of undertakings or institution affiliated to a central body may have a legitimate interest to transmit personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.	
	Amendment 16		
(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities,	(39) The processing of data to the extent strictly necessary ***and proportionate*** for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist~~, at a given level of confidence,~~ accidental events or ~~unlawful or~~ malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by~~, or accessible via,~~ these networks and systems, by public	(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities,	(39) The processing of data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security constitutes a legitimate interest of the controller concerned.

Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.	authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. ***This principle also applies to processing of personal data to restrict abusive access to and use of publicly available network or information systems, such as the blacklisting of electronic identifiers.***	Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams - – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the ~~concerned~~ data controller **concerned**. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. ***The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.***	

	Amendment 17		
	(39a) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the prevention or limitation of damages on the side of the data controller should be presumed as carried out for the legitimate interest of the data controller or, in case of disclosure, of the third party to whom the data ~~is~~ are disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller. The same principle also applies to the enforcement of legal claims against a data subject, such as debt collection or civil damages and remedies.		

	Amendment 18		
	(39b) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the processing of personal data for the purpose of direct marketing for own or similar products and services or for the purpose of postal direct marketing should be presumed as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data are disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller if highly visible information on the right to object and on the source of the personal data is given. The processing of business contact details should be generally regarded as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data are disclosed, and as meeting the		

	reasonable expectations of the data subject based on his or her relationship with the controller. The same should apply to the processing of personal data made manifestly public by the data subject.		
	Amendment 19		
(40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this	***deleted***	(40) The processing of personal data for other purposes ***than the purposes for which the data have been initially collected*** should be only allowed where the processing is compatible with those purposes for which the data have been initially collected~~,~~**.** ~~in~~ **In** ***such case no separate legal basis is required other than the one which allowed the collection of the data. If*** ~~particular where~~ the 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, Union law or Member State law may determine and specify the tasks and purposes for which the further processing shall be regarded as lawful. The further processing for archiving purposes***	(40) Further processing of personal data where this is necessary for historical, statistical or scientific purposes, or for purposes of archiving in the public interest is not to be considered incompatible with the purposes for which the data have previously been processed, subject to the provision of appropriate safeguards; these safeguards must effectively ensure in particular that the data cannot be used in support of measures or decisions regarding any particular individual, except for those measures or decisions specifically foreseen in Member State law, in particular, with regard to archiving in the public interest.

Regulation and in particular the information of the data subject on those other purposes should be ensured.		***in the public interest, or*** ~~historical~~, statistical**,** ~~or~~ scientific ~~**research**~~ **or historical** purposes ***or in view of future dispute resolution should be considered as compatible lawful processing operations***. ***The legal basis provided by Union or Member State law for the collection and processing of personal data may also provide a legal basis for further processing for other purposes if these purposes are in line with the assigned task and the controller is entitled legally to collect the data for these other purposes.*** ***In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account inter alia any link between those purposes and the purposes of the intended further processing, the context in which the data have been collected, including the reasonable expectations of the data subject as to their further use, the nature of the personal data, the***	

		consequences of the intended further processing for data subjects, and the existence of appropriate safeguards in both the original and intended processing operations. Where the ***intended*** other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes ***and on his or her rights including the right to object,*** should be ensured. ***Indicating possible criminal acts or threats to public security by the controller and transmitting these data to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However such transmission in the legitimate interest of the controller***	

		or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.	

	Amendment 20		
(41) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.	***deleted***	(41) Personal data which are, by their nature, particularly sensitive ~~and vulnerable~~ in relation to fundamental rights ***and freedoms*** ~~or privacy~~, deserve specific protection ***as the context of their processing may create important risks for the fundamental rights and freedoms. These data should also include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races.*** Such data should not be processed, unless ***processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the***	(41) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his or her explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing.

		specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided inter alia where the data subject gives his ***or her*** explicit consent. ~~However, derogations from this prohibition should be explicitly provided for~~ ***or*** in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms. ***Special categories of personal data may also be processed where the data have manifestly been made public or voluntarily and at the request of the data subject transferred to the controller for a specific purpose specified by the data subject, where the processing is done in the interest of the data subject.***	

		Member State and Union Law may provide that the general prohibition for processing such special categories of personal data in certain cases may not be lifted by the data subject's explicit consent.	

	Amendment 21		
(42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.	(42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, for historical, statistical and scientific research purposes***, or for archive services***.	(42) Derogating from the prohibition on processing sensitive categories of data should also be allowed ~~if done by a~~ ***when provided for in Union or Member State*** law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify***, in particular*** **processing data** ***in the field of employment law, social security and social protection law, including pensions and*** **for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health or ensuring high standards of quality and safety of health care and services and of medicinal products or medical devices or assessing public policies adopted in the field of health, also by producing quality and activity indicators.** and in ~~particular~~ ***This may be done*** for health purposes, including public health ~~and social protection~~ and the management of health-care	(42) Derogating from the prohibition on processing sensitive categories of data should also be allowed when provided for in Union or Member State law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify.

		services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for ***archiving in the public interest or*** historical, statistical and scientific ~~research~~ purposes. ***A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.***	

		(42a) **Special categories of personal data which deserve higher protection, may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health or social care services** ***and systems including the processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system,*** **and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes or for archiving purposes in the public interest, for historical, statistical or scientific purposes as well as for studies conducted in the public interest in the area of public health. Therefore this Regulation**	

		should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of individuals.	
		(42b) The processing of special categories* of *personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. This processing is subject to suitable and specific measures so as to protect the rights and freedoms of individuals. In that context, 'public health' should be interpreted as defined in	
		Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public	

		health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.	
(43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.	(43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.	(43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.	

(44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.	(44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.	(44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.	
	Amendment 22		
(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. In case of a request for access, the controller should be entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks.	(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. In case of a request for access, the controller should be entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks. ***If it is possible for the data subject to provide such data, controllers should not be able to invoke a lack of information to refuse an access request.***	(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation~~. In case of a request for access, the controller should be entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks~~ ***However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her***	(45) Where a data subject exercises his or her rights under Articles 15-20 of this Regulation, the controller may request such information from him or her as is necessary in order to locate the personal data requested or to verify that the personal data relate to the individual who submitted the request. The controller, however, shall not request the data subject to reveal his or her name or any other identifying information not already available to the controller, unless it is not possible to carry out the verification via other less intrusive means.

		rights.	
			(45a) Effective rights of the data subject are an important component of the right to the protection of personal data enshrined in Article 8 of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty.
(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.	(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to **him or her** are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.	(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language ***and, additionally, where appropriate, visualisation*** is used. ***This information could be provided in electronic form, for example, when addressed to the public, through a website.*** This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any	(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. In particular, the data subject must know and understand if personal data relating to him or her are being collected, by whom and for what purpose to the extent that he or she is able to be in control of the personal data. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in a clear and plain language that the child can easily understand.

		information and communication, where processing is addressed ~~specifically~~ to a child, should be in such a clear and plain language that the child can easily understand.	
	Amendment 23		
(47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.	(47) Modalities should be provided for facilitating the data subject's exercise of **his or her** rights provided by this Regulation, including mechanisms to ~~request~~ ***obtain***, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a ~~fixed~~ ***reasonable*** deadline and give reasons, in case he does not comply with the data subject's request.	(47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, ~~free of charge,~~ in particular access to data, rectification, erasure and to exercise the right to object. ***Thus the controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means.*** The controller should be obliged to respond to requests of the data subject ***without undue delay and at the latest*** within a fixed deadline ***of one month*** and give reasons ***where the controller*** ~~, in case he~~ does not ***intend to*** comply with the data subject's request.	(47) Modalities should be provided for facilitating the data subject's exercise of his or her rights provided by this Regulation, including mechanisms to obtain, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a reasonable deadline and give reasons, in case he does not comply with the data subject's request.
			(47a) The controller should use all reasonable measures to verify the identity of a data subject that makes

			a request in the exercise of the rights of the data subject, in particular in the context of online services and online identifiers. The notion of identification also includes the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller. A controller should not retain personal data for the sole purpose of being able to react to potential requests.
			(47b) Where a data subject makes a request for rectification, erasure, objection or restriction, the controller should make best efforts to notify each recipient to whom the data have been transferred.

	Amendment 24		
(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.	(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be ***likely*** stored ***for each purpose***, ***if the data are to be transferred to third parties or third countries,*** on the existence ***of measures to object and*** of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data. ***This information should be provided, which can also mean made readily available, to the data subject after the provision of simplified information in the form of standardised icons. This should also mean that personal data are processed in a way that effectively allows the data subject to exercise his or her rights.***	(48) The principles of fair and transparent processing require that the data subject should be informed ~~in particular~~ of the existence of the processing operation and its purposes~~, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint.~~ ***The controller should provide the data subject with any further information necessary to guarantee fair and transparent processing. Furthermore the data subject should be informed about the existence of profiling, and the consequences of such profiling.*** Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.	(48) The principles of fair and transparent processing require that the data subject should be informed about the relevant details of the processing operation, in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the rights of access, rectification or erasure and on the right to lodge a complaint. The data subject has the right to receive information, irrespective of whether data are collected directly from him or her, or from other sources.

(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.	(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.	(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient. ***Where the controller intends to process the data for a purpose other than the one for which the data were collected the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the data could not be provided to the data subject because various sources have been used, the information should be provided in a general manner.***	

	Amendment 25		
(50) However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.	(50) However, it is not necessary to impose this obligation where the data subject already ~~disposes of~~ ***knows*** this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. ~~The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.~~	(50) However, it is not necessary to impose this obligation where the data subject already ~~disposes~~ ***possesses*** ~~of~~ this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for ***archiving purpose in the public interest, for*** historical, statistical or scientific ~~research~~purposes; in this regard, the number of data subjects, the age of the data, and any ~~compensatory measures~~ ***appropriate safeguards*** adopted may be taken into consideration.	

	Amendment 26		
(51) 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.	(51) Any person should have the right of access to data which have 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 ***estimated*** period, which recipients receive the data, what is the ***general*** 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~~***, such as in relation to*** the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	(51) ~~Any~~ ***A natural*** person should have the right of access to data which has been collected concerning ~~them~~**him or her**, and to exercise this right easily ***and at reasonable intervals***, in order to be aware ***of*** and verify the lawfulness of the processing. **This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.** Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, ***where possible*** for what period, which recipients receive the data, what is the logic ***involved in any automatic*** ~~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	(51) Any person should have the right of access to data which have been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. The data undergoing processing should be communicated in an intelligible form and without an excessive charge, which should not exceed the cost of providing such data.

		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. ***Where the controller processes a large quantity of information concerning the data subject, the controller may request that before the information is delivered the data subject specify to which information or to which processing activities the request relates.***	

(52) The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	(52) The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	(52) The controller should use all reasonable measures to verify the identity of a data subject ~~that~~***who*** requests access, in particular in the context of online services and online identifiers. ***Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-into the on-line service offered by the data controller.*** A controller should not retain personal data for the ~~unique~~ ***sole*** purpose of being able to react to potential requests.	

	Amendment 27		
(53) Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it	(53) Any person should have the right to have personal data concerning them rectified and a 'right to ~~be forgotten~~ ***erasure***' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. ~~This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.~~ However, the further retention of the data should be allowed where it	(53) ~~Any~~ ***A natural*** person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation ***or with Union or Member State law to which the controller is subject***. 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~~ ***in particular*** 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. ***The data subject should be able to***	(53) Any person should have the right to have personal data concerning them rectified and a right to erasure where the retention of such data is not in compliance with this Regulation.

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.	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. ***Also, the right to erasure should not apply when the retention of personal data is necessary for the performance of a contract with the data subject, or when there is a legal obligation to retain this data.***	***exercise this right notwithstanding the fact that he or she is no longer a child.*** However, the further retention of the data should be ~~allowed~~ ***lawful*** 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 ***and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,*** **for reasons of public interest in the area of public health,** ***for archiving purposes in the public interest,*** **for historical, statistical and scientific purposes** ***or for the establishment, exercise or defence of legal claims*** ~~when required by law or where there is a reason to restrict the processing of the data instead of erasing them~~.	

	Amendment 28		
(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.	(54) To strengthen the 'right to ~~be forgotten~~ ***erasure***' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public ***without legal justification*** 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~~ ***take all necessary steps to have the data erased, including by third parties, without prejudice to the right of the data subject to claim compensation.***	(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform ~~third parties~~ ***the controllers*** 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~~ **the** ***above mentioned*** information, the controller should take ~~all~~reasonable steps, ***taking into account available technology and the means available to the controller,*** including technical measures, in relation to data for the publication of which the controller is responsible. ~~In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.~~	(54) To strengthen the right to erasure in the online environment, a controller who unlawfully processes personal data made publicly available should be obliged to take all necessary steps to have the data de-listed or erased, including by third parties, without prejudice to the right of the data subject to claim compensation.

	Amendment 29		
	(54a) Data which are contested by the data subject and whose accuracy or inaccuracy cannot be determined should be blocked until the issue is cleared.		(54a) Individuals may need their personal data to be further processed even if the conditions for erasure are met. In this situation, the processing of the data should be restricted, solely following the request of the data subject.
		54a) Methods to restrict processing of personal data could include, inter alia, temporarily moving the selected data to another processing system or making the selected data unavailable to users or temporarily removing published data from a website. In automated filing systems the restriction of processing of personal data should in principle be ensured by technical means; the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data is restricted.	

	Amendment 30		
(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.	(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. ***Data controllers should be encouraged to develop interoperable formats that enable data portability.*** This should apply where the data subject provided the data to the automated processing system, based on ~~their~~***his or her*** consent or in the performance of a contract. ***Providers of information society services should not make the transfer of those data mandatory for the provision of their services.***	(55) To further strengthen the control over their own data ~~and their right of access, data subjects should have the right,~~ where ***the processing of*** personal data ~~are processed~~ ***is carried out*** by ~~electronic~~ ***automated*** means ~~and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The~~ **the** data subject should also be allowed to ~~transmit~~ ***receive*** ~~those~~ ***the personal*** data ***concerning him or her***, which ~~they have~~ ***he or she has*** provided ~~,~~ ~~from one automated application, such as a social network, into~~ ***to a controller, in a structured and commonly used and machine-readable format and transmit to*** another ~~one~~***controller***. This ***right*** should apply where the data subject provided the ***personal*** data ~~to the automated processing system,~~ based on ~~their~~ ***his or her*** consent or in the performance of a contract***. It should not apply where processing is based on another legal ground other than consent or***	(55) To further strengthen the control over their own data and their right of access, data subjects should have the right to obtain the transmission to another controller of the data relating to them, in a format that can be further used, and the right to obtain themselves the data in such a format. Controllers should be encouraged to develop interoperable formats that enable data portability.

		contract. By its very nature this right should not be exercised against controllers processing data in the exercise of their public duties. It should therefore in particular not apply where processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. ***The data subject's right to transmit personal data does not create an obligation for the controllers to adopt or maintain data processing systems which are technically compatible.*** ***Where, in a certain set of personal data, more than one data subject is concerned, the right to transmit the data should be without prejudice to the requirements on the lawfulness of the processing of personal data related to another data subject in accordance with this Regulation. This right should also not prejudice the right of the data subject to obtain the erasure***	

		of personal data and the limitations of that right as set out in this Regulation and should in particular not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract.	

	Amendment 31		
(56) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.	(56) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to ~~them~~***him or her, free of charge and in a manner that can be easily and effectively invoked***. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.	(56) In cases where personal data might lawfully be processed ~~to protect the vital interests of the data subject, or~~ ***because 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 or*** on grounds of ~~public interest, official authority or~~ the legitimate interests of a controller ***or a third party***, any data subject should nevertheless be entitled to object to the processing of any data relating to ~~them~~***their particular situation***. ~~The burden of proof~~ ***It*** should be ~~on~~ ***for*** the controller to demonstrate that their ***compelling*** legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.	(56) In cases where personal data might lawfully be processed, in particular to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object, free of charge, to the processing of any data relating to their particular situation. The burden of proof should be on the controller to demonstrate compelling legitimate grounds that may override the interests or the fundamental rights and freedoms of the data subject.

	Amendment 32		
(57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked.	(57) Where ~~personal data are processed for the purposes of direct marketing,~~ the data subject ~~should have~~ ***has*** the right to object to ~~such~~ ***the*** processing ~~free of charge and in a manner that can be easily and effectively invoked~~***, the controller should explicitly offer it to the data subject in an intelligible manner and form, using clear and plain language and should clearly distinguish it from other information.***	(57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing***, whether the initial or further processing,*** free of charge and in a manner that can be easily and effectively invoked.	(57) Where personal data are processed for the purposes of marketing, the data subject should have the right to object to such processing, free of charge and in a manner that can be easily and effectively invoked.
			(57a) A restriction of processing of personal data may take place by, *inter alia*, temporarily moving the selected data to another processing system or making the selected data unavailable to users or temporarily removing published data from a website. The existence of a restriction should be made clearly visible to the persons in charge of the processing of personal data.

	Amendment 33		
(58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.	(58) ***Without prejudice to the lawfulness of the data processing, every*** natural person should have the right ~~not to be subject~~ ***to object*** to ~~a measure which is based on~~ profiling ~~by means of automated processing. However, such measure~~***. Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject*** should ***only*** be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. ~~The~~ 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~~ ***assessment*** and that such measure should not concern a child. ***Such measures should not lead to discrimination against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union***	(58) ~~Every natural person~~ ***The data subject*** should have the right not to be subject to a ~~measure~~ ***a decision evaluating personal aspects relating to him or her*** which is based ***solely*** on ~~profiling by means of~~ automated processing***, which produces legal effects concerning him or her*** ***or significantly affects him or her, like automatic refusal of an on-line credit application or e-recruiting practices without any human intervention***. ***Such processing includes also 'profiling' consisting in any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements as long as it produces legal effects concerning him or her or significantly affects him or her.*** However, ~~such measure~~ ***decision making based on such processing, including profiling,*** should be allowed when ~~expressly~~ authorised	(58) Every natural person should have the right not to be subject to a measure which is based solely or predominantly on profiling by means of automated processing. Where the natural person is subject to such a measure, following the derogations allowed by this Regulation, the controller must have in place suitable safeguards. In order to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed, the controller should implement adequate procedures for the profiling and technical and organisational measures appropriate to ensure in particular that factors which result in data inaccuracies are corrected and the risk of errors is minimized, secure personal data in a way which takes account of the potential risks involved for the interests and rights of the data subject.

	membership, sexual orientation or gender identity.	by ***Union or Member State*** law~~,~~ ~~carried out in the course of~~ ***to which the controller is subject, including for fraud and tax evasion monitoring and prevention purposes and to ensure the security and reliability of a service provided by the controller, or necessary for the*** entering or performance of a contract ***between the data subject and a controller***, or when the data subject has given his ***or her explicit*** 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~~, ***to express his or her point of view, to get an explanation of the decision reached after such assessment and the right to contest the decision. In order to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed, the controller should use adequate mathematical or statistical procedures for the profiling, implement technical and***	

		organisational measures appropriate to ensure in particular that factors which result in data inaccuracies are corrected and the risk of errors is minimized, secure personal data in a way which takes account of the potential risks involved for the interests and rights of the data subject and which prevents inter alia discriminatory effects against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic or health status, sexual orientation or that result in measures having such effect. Automated decision making and profiling based on special categories of personal data should only be allowed under specific conditions.	

	Amendment 34		
	(58a) Profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests, rights or freedoms of the data subject. Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous.		
		(58a) Profiling as such is subject to the (general) rules of this Regulation governing processing of personal data (legal grounds of processing, data protection principles etc.) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual). The European Data Protection Board should have the possibility to issue guidance in this context.	

	Amendment 35		
(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	(59) Restrictions on specific principles and on the rights of information, ~~access,~~ rectification and erasure or on the right ***of access and*** to ***obtain*** 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 ***specific and well-defined*** 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.	(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, ***the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political***	(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, for the purposes enshrined in Article 21 of this Regulation. Any such legislative measure shall contain the specific safeguards ennumerated in Article 21(2) of this Regulation in order to be considered necessary and proportionate in a democratic society. 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.

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.	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.	***behaviour under former totalitarian state regimes*** or the protection of the data subject or the rights and freedoms of others**,** ***including social protection public health and humanitarian purposes, such as the performance of a task incumbent upon the International Red Cross and Red Crescent Movement***. 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.	
		(59a) Nothing in this Regulation should derogate from the privilege of non-disclosure of confidential information of the International Committee of the Red Cross under international law, which shall be applicable in judicial and administrative proceedings.	

	Amendment 36		
(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation.	(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established***, in particular with regard to documentation, data security, impact assessments, the data protection officer and oversight by data protection authorities***. In particular, the controller should ensure and be ~~obliged~~ ***able*** to demonstrate the compliance of each processing operation with this Regulation. ***This should be verified by independent internal or external auditors.***	(60) ~~Comprehensive~~ ***The*** responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ~~ensure and~~ be obliged ***to implement appropriate measures and be able*** to demonstrate the compliance of ~~each~~ processing ~~operation~~ ***activities*** with this Regulation. ***These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals.***	(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate measures and be able to demonstrate the compliance of processing operations with this Regulation. These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals and the type of the organisation.
		(60a) Such risks, of varying likelihood and severity, may result from data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymisation, or	

		any other significant economic or social disadvantage; or where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable individuals, in particular of children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects.	

		(60b) **The likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. Risk should be evaluated on an objective assessment, by which it is established whether data processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of individuals.**	
		(60c) Guidance for the implementation of appropriate measures, and for demonstrating the compliance by the controller or processor, especially as regards the identification of the risk related to the processing, their assessment in terms of their origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer. The European Data Protection Board may also	

		issue guidelines on processing operations that are considered to be unlikely to result in a high risk for the rights and freedoms of individuals and indicate what measures may be sufficient in such cases to address such risk.	
	Amendment 37		
(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.	(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. ***The principle of data protection by design requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its***	(61) The protection of the rights and freedoms of ~~data subjects~~ ***individuals*** with regard to the processing of personal data require that appropriate technical and organisational measures are taken, ~~both at the time of the design of the processing and at the time of the processing itself,~~ to ensure that the requirements of this Regulation are met. In order to ~~ensure and~~***be able to*** demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. ***Such measures could consist inter alia of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency***	(61) The protection of the rights and freedoms of individuals with regard to the processing of personal data requires that appropriate technical and organisational solutions designed to implement data protection principles in an effective way and to integrate the necessary safeguards into the processing tools are adopted, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. When ensuring that, by default, personal data are processed in the least intrusive manner, the controller should in particular take into account the nature and amount of data collected, the extent of their processing, the period of their

	ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.	***with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.***	storage and their accessibility.

	Amendment 38		
(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.	(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 arrangement between the joint controllers should reflect the joint controllers' effective roles and relationships. The processing of personal data under this Regulation should include the permission for a controller to transmit the data to a joint controller or to a processor for the processing of the data on ~~their~~ his or her behalf.***	(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor**s**, 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.	(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 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. Joint controllers should conclude arrangements that duly reflect their respective roles and relationships vis-à-vis data subjects.

	Amendment 39		
(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.	(63) Where a controller not established in the Union is processing personal data of data subjects ~~residing~~ in the Union ~~whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour~~, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the ~~controller is a small or medium sized enterprise or~~ ***processing relates to fewer than 5000 data subjects during any consecutive 12-month period and is not carried out on special categories of personal data, or is*** a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.	(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring ***of*** their behaviour ***in the Union***, the controller should designate a representative, unless **the processing it carries out is occasional and unlikely to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing or** the controller is ~~established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or~~ a public authority or body ~~or where the controller is only occasionally offering goods or services to such data subjects~~. The representative should act on behalf of the controller and may be addressed by any supervisory authority**.** ***The representative should be explicitly designated by a written mandate of***	(63) Where a controller not established in the Union is processing personal data of data subjects in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of such data subject, the controller should designate a representative, unless the processing it carries out is occasional and unlikely to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing, or the controller is a public authority or body. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

		the controller to act on its behalf with regard to the latter's obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller under this Regulation. Such representative should perform its tasks according to the received mandate from the controller, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subjected to enforcement actions in case of non-compliance by the controller.	
		(63a) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which	

		will meet the requirements of this Regulation, including for the security of processing. Adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk for the rights and freedoms of the data subject. ***The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency***	

		mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.	
	Amendment 39		
(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.	(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects ~~residing~~ in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.	***deleted***	(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities. The processing of personal data concerning special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems should be regarded as likely to result in a risk for the rights and freedom of individuals.

	Amendment 41		
(65) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	(65) In order to ***be able to*** demonstrate compliance with this Regulation, the controller or processor should ~~document each processing operation~~ ***maintain the documentation necessary in order to fulfill the requirements laid down in this Regulation***. 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~~ ***evaluating the compliance with this Regulation***. ***However, equal emphasis and significance should be placed on good practice and compliance and not just the completion of documentation.***	(65) In order to demonstrate compliance with this Regulation, the controller or processor should ~~document each~~ ***maintain records regarding all categories of*** processing ~~operation~~***activities under its responsibility***. Each controller and processor should be obliged to co-operate with the supervisory authority and make ~~this documentation~~***these records***, on request, available to it, so that it might serve for monitoring those processing operations.	(65) In order to demonstrate compliance with this Regulation, the controller or processor should maintain an inventory of all processing operations under its responsibility. Each controller and processor should be obliged to co-operate with the supervisory authority and make the inventory, on request, available to it, so that it might serve for evaluating the compliance with this Regulation. The inventory should be regarded as a mapping tool facilitating the compliance mechanism.

	Amendment 42		
(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.	(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, ~~the Commission should promote~~ technological neutrality, interoperability and innovation ***should be promoted*** and, where appropriate, ~~cooperate~~ ***cooperation*** with third countries ***should be encouraged.***	(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security ***including confidentiality***, taking into account ***available technology*** ~~the state of the art~~ and the costs of ~~their~~ implementation in relation to the risk~~s~~ and the nature of the personal data to be protected. ~~When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third ***countries***~~ ***In assessing data security risk, consideration should be given to the risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise***	(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, technological neutrality, interoperability and innovation should be promoted and, where appropriate, cooperation with third countries should be encouraged.

		processed, which may in particular lead to physical, material or moral damage.	
		(66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. ***Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should***	

		take place prior to the processing.	
	Amendment 43		
(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to	(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, ~~as soon as the controller becomes aware that such a breach has occurred,~~ the controller should notify the breach to the supervisory authority without undue delay ~~and, where feasible, within 24~~***,which should be presumed to be not later than 72*** hours. ~~Where this cannot achieved within 24 hours~~ ***If applicable***, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud,	(67) A personal data breach may, if not addressed in an adequate and timely manner, result in ***physical, material or moral damage to individuals such*** ~~***as***~~ ~~substantial economic~~ loss ***of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or*** ~~and~~ social ~~harm, including identity fraud,~~ ***disadvantage*** to the individual concerned. Therefore, as soon as the controller becomes aware that ~~such~~ a ***personal data*** breach ***which may result in physical, material or moral damage*** has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within ~~24~~ **72** hours. Where this cannot ***be*** achieved within ~~24~~ **72** hours, an explanation of the reasons	(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that a breach, which is likely to result in a risk for the rights and freedoms of individuals has occurred, the controller should notify the breach to the supervisory authority without undue delay and, no later than 72 hours after having become aware of it. The individuals whose personal data are likely to be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The

reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.	physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach ***and formulate*** ~~as well as~~ recommendations ~~as well as recommendations~~ for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.	for the delay should accompany the notification. The individuals whose ***rights and freedoms*** ~~personal data~~ could be ~~adversely~~ ***severely*** affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. ~~A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation.~~ The notification should describe the nature of the personal data breach as well as recommendations ~~as well as recommendations~~ for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the ~~chance for data subjects~~ ***need*** to mitigate an immediate risk of ~~harm~~***damage*** would call for a prompt notification of data subjects whereas the need to	notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

		implement appropriate measures against continuing or similar data breaches may justify a longer delay.	

(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.	(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.	(68) ~~In order to determine~~ ***It must*** ~~whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should~~ be ascertained whether ~~the controller has implemented and applied~~ ***all*** appropriate technological protection and organisational measures ***have been implemented*** to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject~~.,~~ ~~before a damage to personal and economic interests occurs,~~ ***The fact that the notification was made without undue delay should be established*** taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. ***Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.***	(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

		(68a) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting the personal data .	
(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of	(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law	(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law	(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of

law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.
(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with	(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with	(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation**s** should be abolished, and replaced by effective procedures and mechanism**s** which focus instead on those ***types of*** processing operations which are likely to ~~present specific~~***result in a high*** risk~~s~~ to the rights and freedoms of ~~data subjects~~***individuals*** by virtue of their nature, ~~their~~ scope***, context and*** ~~or their~~ purposes. ~~In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the~~ ***types of*** processing***, operations may be those*** which ~~should include~~ in particular***, involve using new technologies, or are of a new kind***	(70) Processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes should be subject to data protection impact assessment by the controller. Data protection impact assessment should be carried out prior to the processing and should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

this Regulation.	this Regulation.	***and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing***~~the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation~~.	
		(70a) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk, which should	

		include in particular the envisaged measures, safeguards and mechanisms for mitigating that risk and for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.	
(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.	(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.	(71) This should in particular apply to ~~newly established~~ large-scale ~~filing systems~~***processing operations***, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects ***and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk for the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made in cases***	(71) The requirement to conduct data protection impact assessment should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects but should not be limited to them.

		where data are processed for taking decisions regarding specific individuals following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk for the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. **The processing of personal data irrespective of the volume or the nature of the data, should not be considered as being on a large scale, if the processing of these data is protected by**	

		professional secrecy, such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney. In these cases a data protection impact assessment should not be mandatory.	
	Amendment 44		
	(71a) Impact assessments are the essential core of any sustainable data protection framework, making sure that businesses are aware from the outset of all possible consequences of their data processing operations. If impact assessments are thorough, the likelihood of any data breach or privacy-intrusive operation can		

	be fundamentally limited. Data protection impact assessments should consequently have regard to the entire lifecycle management of personal data from collection to processing to deletion, describing in detail the envisaged processing operations, the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure compliance with ~~the~~ this R~~r~~regulation.		
	Amendment 45		
	(71b) Controllers should focus on the protection of personal data throughout the entire data lifecycle from collection to processing to deletion by investing from the outset in a sustainable data management framework and by following it up with a comprehensive compliance mechanism.		

(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.	(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.	(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.	(72) There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.
	Amendment 46		
(73) Data protection impact assessments should be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.	***deleted***	(73) Data protection impact assessments ~~should~~ ***may*** be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.	

	Amendment 47		
(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.	(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, ***the data protection officer or*** the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. ~~Such~~ ***A*** consultation ***of the supervisory authority*** should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.	(74) Where a data protection impact assessment indicates that ***the*** processing ***would, despite the envisaged safeguards, security measures and mechanisms to mitigate the*** ~~operations involve a high degree of specific~~ risk~~s to the~~ ***result in a high risk to the*** rights and freedoms of ~~data subjects~~***individuals and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation***, ~~such as excluding individuals from their right, or by the use of specific new technologies,~~ the supervisory authority should be consulted, prior to the start of ~~operations~~***processing activities***~~, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of~~	(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and may make proposals to remedy such situation.

		~~the processing and lays down appropriate safeguards~~. ***Such high risk is likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the data subject. The supervisory authority should respond to the request for consultation in a defined period. However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of this consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue pursuant to Article 33 may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk for the rights and freedoms of individuals.***	

	Amendment 48		
	(74a) Impact assessments can only be of help if controllers make sure that they comply with the promises originally laid down in them. Data controllers should therefore conduct periodic data protection compliance reviews demonstrating that the data processing mechanisms in place comply with assurances made in the data protection impact assessment. It should further demonstrate the ability of the data controller to comply with the autonomous choices of data subjects. In addition, in case the review finds compliance inconsistencies, it should highlight these and present recommendations on how to achieve full compliance.		

		(74a) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.	(74a) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.
		(74b) A consultation with the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.	

	Amendment 49		
(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently.	(75) Where the processing is carried out in the public sector or where, in the private sector, processing ~~is carried out by a large enterprise~~ ***relates to more than 5000 data subjects within 12 months***, or where its core activities, regardless of the size of the enterprise, involve processing operations ***on sensitive data, or processing operations*** which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. ***When establishing whether data about a large number of data subjects are processed, archived data that are restricted in such a way that they are not subject to the normal data access and processing operations of the controller and can no longer be changed should not be taken into account.*** Such data protection officers, whether or not an employee of the controller ***and whether or not performing that task full time***, should be in a position to perform their duties and	(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person ~~should~~ ***with expert knowledge of data protection law and practices may*** assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks ***in an*** independent~~ly~~ ***manner***.	(75) A data protection officer should assist the controller or processor in the public sector or where, in the private sector, the core activities of an enterprise consist of processing operations which imply regular or systematic monitoring of data subjects or a high level of risk. This is the case notably when the core activities involve the processing of special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems. The resources provided by the controller or processor to the data protection officer shall include the possibility to maintain his or her specialised knowledge. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

	tasks independently ***and enjoy special protection against dismissal. Final responsibility should stay with the management of an organisation. The data protection officer should in particular be consulted prior to the design, procurement, development and setting-up of systems for the automated processing of personal data, in order to ensure the principles of privacy by design and privacy by default.***		
	Amendment 50		
	(75a) The data protection officer should have at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organisational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data		

	security; industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed; the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation. The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee.		

	Amendment 51		
(76) Associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors.	(76) Associations or other bodies representing categories of controllers should be encouraged***, after consultation of the representatives of the employees,*** to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors. ***Such codes should make compliance with this Regulation easier for industry.***	(76) Associations or other bodies representing categories of controllers ***or processors*** should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors ***and the specific needs of micro, small and medium enterprises. In particular such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of individuals***.	(76) Associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics and risks of the processing carried out in certain sectors and identifying best practices. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller and as an element to demonstrate that a selected processor provides sufficient guarantees regarding the compliance with this Regulation.

		(76a) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult with relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.	
	Amendment 52		
(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.	(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and ***standardised*** marks should be encouraged, allowing data subjects to quickly**,** ***reliably and verifiably*** assess the level of data protection of relevant products and services. ***A "European Data Protection Seal" should be established on the European level to create trust among data subjects, legal certainty for controllers, and at the same time export European data protection standards by allowing***	(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.	(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

	non-European companies to more easily enter European markets by being certified.		
(78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.	(78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.	(78) Cross-border flows of personal data ***to and from countries outside the Union and international organisations*** are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to ***controllers, processors or other recipients in*** third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined***, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation.*** In any event, transfers to third countries ***and international organisations*** may only be carried out in full compliance with this Regulation. ***A transfer may only take place if,***	(78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors in third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country.

		subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.	
	Amendment 53		
(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.	(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects ***ensuring an adequate level of protection for the fundamental rights of citizens.***	(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. ***Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of EU law and include safeguards to protect the rights of the data subjects.***	(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of EU law and include an appropriate level of protection for the fundamental rights of the data subjects.
	Amendment 54		
(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international	(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international	(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a ~~processing~~ ***specified*** sector***, such as the private sector or one or***	(80) The Commission may decide with effect for the entire Union that certain third countries, or one or more territories or specified sectors within that third country or the

organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.	organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. ~~In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.~~ ***The Commission may also decide, having given notice and a complete justification to the third country, to revoke such a decision.***	***more specific economic sectors*** within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations, which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.	international organisation in question, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation. The Commission may also decide, having given notice and a complete justification to the third country, to revoke such a decision. Before adopting a decision, the Commission shall consult the European Data Protection Board and provide it with all necessary documentation.

(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.	(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.	(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of ~~the~~**a** third country ***or of a territory or of a specified sector within a third country***, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards ***and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision to a territory or a specified sector in a third country should take into account clear and objective criteria , such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees that ensure an adequate level of protection in particular when data are processed in one or several specific sectors.*** ***In particular, the third country should ensure effective data***	(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or of a specified sector within a third country or international organisation, take into account the respect for the rule of law, access to justice as well as international human rights norms and standards and their general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision should take into account clear and objective criteria, such as respect for the core data protection principles in particular relating to purpose limitation, data quality and proportionality principle, transparency principle, security principle, rights of access, rectification, and erasure, the restrictions on onward transfers. In particular, the third country should ensure effective independent data protection

		protection supervision and should provide for cooperation mechanisms with the European data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.	supervision and should provide for cooperation mechanisms with the supervisory authorities in the Union, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.
		(81a) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the	

		Automatic Processing of Personal Data and its Additional Protocol **should be taken into account.** ***The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations.***	
		(81b) The Commission should monitor the functioning of decisions on the level of protection in a third country or a territory or specified sector within a third country, or an international organisation, including decisions adopted on the basis of Article 25(6) or Article 26 (4) of Directive 95/46/EC. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any pertinent findings to the Committee within the meaning of Regulation (EU) No 182/2011 as established under this Regulation.	(81b) The Commission should monitor the functioning of decisions on the level of protection in a third country or a territory or specified sector within a third country, or an international organisation, including decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. The Commission should evaluate, within a five-year period, the functioning of the decisions and report any pertinent findings to the Committee referred to in Article 87 of this Regulation.

	Amendment 55		
(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.	(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. ***Any legislation which provides for extra-territorial access to personal data processed in the Union without authorisation under Union or Member State law should be considered as an indication of a lack of adequacy.*** Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.	(82) The Commission may ~~equally~~ recognise that a third country, or a territory or a ~~processing~~ ***specified*** sector within a third country, or an international organisation ~~offers~~ no ***longer ensures an*** adequate level of data protection. Consequently the transfer of personal data to that third country ***or international organisation*** should be prohibited, ***unless the requirements of Articles 42 to 44 are fulfilled***. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. ***The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation***.	(82) The Commission may equally recognise that a third country or international organisation, or a territory or a processing sector within a third country or international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.

	Amendment 56		
(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority.	(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority~~, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority~~. ***Those appropriate safeguards should uphold a respect of the data subject's rights adequate to intra-EU processing, in particular relating to purpose limitation, right to access, rectification, erasure and to claim compensation. Those safeguards should in particular guarantee the***	(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or ***ad hoc*** contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. ***Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. They should relate in particular to compliance with the general principles relating***	(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the European Data Protection Board or by a supervisory authority in accordance with the consistency mechanism referred to in Article 57, or contractual clauses authorised by the competent supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to intra-EU processing in particular relating to purpose limitation, data quality and proportionality principle, transparency principle, security principle, rights of access, rectification, and erasure, the restrictions on onward transfers, as well as including the right to

	observance of the principles of personal data processing, safeguard the data subject's rights and provide for effective redress mechanisms, ensure the observance of the principles of data protection by design and by default, guarantee the existence of a data protection officer.	***to personal data processing, the availability of enforceable data subject's rights and of effective legal remedies and the principles of data protection by design and by default. Transfers may be carried out also by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding. The authorisation of the competent supervisory authority should be obtained when the safeguards are adduced in non legally binding administrative arrangements.***	enforce data subjects' rights and of effective legal remedies, including the right to obtain effective administrative or judicial redress and to claim compensation. Authorisations by Member States or supervisory authorities adopted prior to the entry into force of this Regulation shall remain valid until amended, replaced or repealed by that Member State or supervisory authority. Consistency with this Regulation should be assessed where appropriate.

	Amendment 57		
(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses ***or supplementary safeguards*** as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted ~~by the Commission or~~ by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. ***The standard data protection clauses adopted by the Commission could cover different situations, namely transfers from controllers established in the Union to controllers established outside the Union and from controllers established in the Union to processors, including sub-processors, established outside the Union. Controllers and processors should be encouraged to provide even more robust safeguards via***	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract***, including in a contract between the processor and another processor,*** nor to add other clauses ***or additional safeguards*** as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the European Data Protection Board or by a supervisory authority in accordance with the consistency mechanism should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the European Data Protection Board or by a supervisory authority, or prejudice the fundamental rights or freedoms of the data subjects.

	additional contractual commitments that supplement standard protection clauses.		
	Amendment 58		
(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.	(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include ***all*** essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data	(85) A corporate group ***or a group of enterprises engaged in a joint economic activity*** should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings ***or group of enterprises***, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.	(85) A group of undertakings or a group of enterprises engaged in a joint economic activity should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings or group of enterprises, as long as such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

	Amendment 59		
(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients***, taking into full account the interests and fundamental rights of the data subject***.	(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his ***explicit*** consent, where the transfer is ~~necessary~~ ***occasional*** in relation to a contract or a legal claim, ***regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers*** where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be	(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies, or where the transfer is necessary to protect the vital interests of the data subject or of other persons, such as in cases of transfers to humanitarian international organisations acting in compliance with humanitarian law applicable in armed conflicts. Provision should also be made for the possibility for transfers where important grounds of public interests laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter

		the recipients.	case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.
	Amendment 60		
(87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences.	(87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters ***or for public health***, or to competent ***public*** authorities for the prevention, investigation, detection and prosecution of criminal offences***, including for the prevention of money laundering and the fight***	(87) These ~~derogations~~ ***rules*** should in particular apply to data transfers required and necessary for ~~the protection of~~ important ~~grounds~~ ***reasons*** of public interest, for example in cases of international data ~~transfers~~ ***exchange*** between competition authorities, tax or customs administrations, ***between*** financial supervisory authorities, between services competent for social security matters, or ~~to competent authorities~~ for ~~the prevention, investigation, detection and prosecution of criminal offences~~***for public health, for example in case of contact tracing***	(87) These derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with the view to accomplishing a

	against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the personal data for such important grounds of public interest should only be used for occasional transfers. In each and every case, a careful assessment of all circumstances of the transfer should be carried out.	***for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organization. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation, such as a National Society of the Red Cross or to the ICRC of personal data of a data subject who is physically or legally incapable of giving consent, with the view to accomplishing a task incumbent upon the International Red Cross and Red Crescent Movement under the Geneva Conventions and/or to work for the faithful application of international***	task incumbent under the Geneva Conventions of 1949 and their amending protocols and/or to work for the faithful application of international humanitarian law applicable in armed conflicts could be considered as necessary for an important reason of public interest or being in the vital interest of the data subject.

		humanitarian law applicable in armed conflicts could be considered as necessary for an important reason of public interest or being in the vital interest of the data subject.	
	Amendment 61		
(88) Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.	(88) ~~Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer.~~ For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.	(88) Transfers which cannot be qualified as ***large scale or*** frequent ~~or massive~~, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when ~~they have~~ ***those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has*** assessed all the circumstances surrounding the data transfer. ***The controller or processor should give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the***	

		situation in the country of origin, the third country and the country of final destination, and adduced suitable safeguards to protect fundamental rights and freedoms of natural persons with respect to processing of their personal data. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. ***To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.***	
	Amendment 62		
(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that	(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a ***legally binding***	(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they	

they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.	guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once those data have been transferred***, to the extent that the processing is not massive, not repetitive and not structural***. ***That guarantee should include financial indemnification in cases of loss or unauthorised access or processing of the data and an obligation, regardless of national legislation, to provide full details of all access to the data by public authorities in the third country.***	will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.	
	Amendment 63		
(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals	(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed	(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed	(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals

guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.	in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act. ***In cases where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the Union on the one hand, and that of a third country on the other, the Commission should ensure that Union law takes precedence at all times. The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question***.	in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. ~~The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.~~	guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may *inter alia* be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. Disclosure of personal data following the request of a court, tribunal or an administrative authority of a third country should only take place in accordance with a mutual legal assistance treaty or international agreement or a relevant legal channel for international cooperation.

(91) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.	(91) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.	(91) When personal data moves across borders ***outside the Union*** it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. ***For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of***	(91) When personal data moves across borders outside the Union it may put at increased risk the ability of individuals to exercise data protection rights, in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. The Commission should take appropriate steps in developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of

		legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.	legislation for the protection of personal data. For these purposes, the competent supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.
	Amendment 64		
(92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.	(92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. ***An authority shall have adequate financial and personal resources to fully carry out its role, taking into account the size of the population and the amount of***	(92) The establishment of supervisory authorities in Member States, ***empowered to perform their tasks and*** ~~exercising~~ ***exercise*** their ~~functions~~ ***powers*** with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.	(92) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Complete independence applies to the authority as such, but also to its members. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

	personal data processing.		
		(92a) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subjected to control or monitoring mechanism regarding their financial expenditure. Neither does it imply that supervisory authorities cannot be subjected to judicial review.	
(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.	(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.	(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.	(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.
	Amendment 65		
(94) Each supervisory authority	(94) Each supervisory authority	(94) Each supervisory authority	(94) Each supervisory authority

should be provided with the adequate financial and human resources, premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.	should be provided with the adequate financial and human resources, ***paying particular attention to ensuring adequate technical and legal skills of staff,*** premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.	should be provided with the ~~adequate~~ financial and human resources, premises and infrastructure, which ~~is~~ ***are*** necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union. ***Each supervisory authority should have a separate annual budget, which may be part of the overall state or national budget.***	should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union. Each supervisory authority should have specific, public, annual budgets which may, where necessary, be part of the budget of another administration, of the overall state or national budget. That budget is subject to financial control which shall not affect its independence.

	Amendment 66		
(95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.	(95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be ~~either~~ appointed by the parliament or the government of the Member State ***taking due care to minimise the possibility of political interference***, and include rules on the personal qualification of the members***, the avoidance of conflicts of interest*** and the position of those members.	(95) The general conditions for the ***member or*** members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament ***and/***or the government ***or the head of State*** of the Member State~~, and include rules on the personal qualification of the members and the position of those~~ ***members or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not.***	(95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be appointed either by the parliament, or the head of State or the government of the Member State concerned, by common accord with the parliament, or by an independent body entrusted by Member State law with the appointment. The Member States should take due care to minimise the possibility of political interference, and include rules on the personal qualification of the members, the avoidance of conflicts of interest and the position of those members. The duration of the term of the member or members of each supervisory authority should not be less than four years. However, such a period may be shorter when a supervisory authority is composed of several members and the renewal of those members is still subject to a procedure that was set

			up before the entry into force of the Regulation.

		(95a) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the European Union when targeting data subjects residing in its territory. This should include dealing with complaints lodged by a data subject, conducting investigations on the application of the Regulation, promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.	(95a) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should include dealing with complaints, conducting investigations on the application of the Regulation, promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.	(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.	(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, ***this Regulation should oblige and empower*** the supervisory authorities ~~should~~ ***to*** co-operate with each other and the Commission***, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation***.	(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other.

	Amendment 67		
(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.	(97) Where the processing of personal data 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~~ ***act as the single contact point and the lead authority responsible for supervising*** the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.	(97) Where the processing of personal data ***takes place*** in the context of the activities of an establishment of a controller or a processor in the Union ***and the controller or processor is established*** ~~takes place~~ in more than one Member State, ***or where processing taking place in the context of the activities of a*** ~~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~~ ***establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should***	(97) Where a transnational 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, one single supervisory authority should act as the single contact point and the lead authority responsible for supervising 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. The lead authority shall be the supervisory authority of the Member State where the main establishment of the controller or processor is situated.

		cooperate with the other authorities that are concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority to which such complaint has been lodged should also be a concerned supervisory authority. Within its tasks to issue guidelines on any question covering the application of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.	

		(97a) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the concerned supervisory authorities in the decision-making process. In cases where the decisions is to reject the complaint by the data subject in whole or in part that decision should be adopted by the supervisory authority at which the complaint has been lodged.	
		(97b) The decision should be agreed jointly by the lead supervisory authority and the concerned supervisory authorities and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure the compliance with this Regulation and the implementation of the decision notified by the lead	

		supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.	
		(97c) Each supervisory authority not acting as lead supervisory authority should be competent to deal with local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involving only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay on this matter. After being informed, the lead supervisory authority should decide, whether it will deal with the case within the one-stop-shop mechanism or whether the supervisory authority which informed it should deal with the case at local level. When deciding whether it will deal with the case,	(97c) Each supervisory authority not acting as lead supervisory authority should be competent to deal with local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and substantially affects only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay on this matter. After being informed, the lead supervisory authority should decide, whether it will deal with the case within the one-stop-shop mechanism or whether the supervisory authority which informed it should deal with the case at local level. When deciding

		the lead supervisory authority should take into account, whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it, in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to deal with the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in the one-stop-shop mechanism.	whether it will deal with the case, the lead supervisory authority should take into account, whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it, in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to deal with the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in the one-stop-shop mechanism.

	Amendment 68		
(98) The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment.	(98) The ~~competent~~ ***lead*** authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment ***or its representative***. ***The European Data Protection Board may designate the lead authority through the consistency mechanism in certain cases at the request of a competent authority.***	(98) The ~~competent~~ ***rules on the lead supervisory*** authority, ~~providing such~~ ***and the*** one-stop-shop ***mechanism***, should ***not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases*** ~~be~~ the ***only*** supervisory authority ***competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority*** of the Member State ***where the public authority or private body is established*** ~~in which the controller or processor has its main establishment~~.	
	Amendment 69		
	(98a) Data subjects whose personal data ~~is~~ are processed by a data controller or processor in another Member State should be able to complain to the supervisory authority of their choice. The lead data protection authority should coordinate its work with that of the other authorities involved.		(98a) Data subjects whose personal data are processed by a controller or processor in another Member State should be able to complain to the supervisory authority of their choice. The lead data protection authority should coordinate its work with that of the other authorities involved.

(99) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.	(99) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.	***deleted***	
(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity	(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union	(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same ~~duties~~ ***tasks*** and effective powers, including powers of investigation, ***corrective powers*** ~~legally binding intervention, decisions~~ and sanctions, ***and authorisation and advisory powers,*** particularly in cases of complaints from individuals, ***and without infringements of this Regulation to prejudice to the powers of***	(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union

with Union law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.	law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.	***prosecutorial authorities under national law, to bring the attention of the judicial authorities*** and***/or*** to engage in legal proceedings. ***Such powers should also include the power to forbid the processing on which the authority is consulted. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in conformity with appropriate procedural safeguards set out in Union law and national law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned.*** ~~Investigative~~ ***Investigatory*** powers ~~of supervisory authorities~~ as regards access to premises should be	law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation. The powers of supervisory authorities should be exercised in conformity with appropriate procedural safeguards set out in Union law and national law, impartially, fairly and within a reasonable time. Each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, and respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken. No costs should be charged by the supervisory authority to individuals in this context.

		exercised in ~~conformity~~ ***accordance with specific requirements in national procedural law, such as*** ~~with Union law and national law. This concerns in particular~~ the requirement to obtain a prior judicial authorisation. ***Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy.*** ***This should not preclude additional requirements pursuant to national procedural law. The adoption of such legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.***	
	Amendment 70		
(101) Each supervisory authority should hear complaints lodged by	(101) Each supervisory authority should hear complaints lodged by	(101 & 101a) ~~Each~~ ***Where the*** supervisory authority ~~should hear~~ ***to***	

any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	any data subject ***or by associations acting in the public interest*** and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject ***or the association*** of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	***which the*** complaint~~s~~ ***has been*** lodged ***is not the lead supervisory authority, the lead supervisory authority should closely co-operate with the supervisory authority to which the complaint has been lodged according to the provisions on co-operation and consistency laid down in this Regulation. In such cases,*** ~~by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case.~~	

		~~The~~***the lead*** supervisory authority should***, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the*** ~~inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another~~ supervisory authority~~, intermediate information should be given to the data subject~~ ***to which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority***.	
		(101b) The supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of the Regulation should seek an amicable settlement and, if this proves unsuccessful, exercise its full range of powers in	

		cases where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the one Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States. This should include specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; or to processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or that has to be assessed taking into account relevant legal obligations under national law.	

(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.	(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.	(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as ~~data subjects~~***individuals in particular in the educational context***.	(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as at individuals, in particular in the educational context. Activities addressed to children should receive specific attention.

			(102a) Where the supervisory authority to which a complaint has been lodged is not the lead supervisory authority, the lead authority should cooperate with the other concerned authority. The other concerned authorities are the supervisory authorities of the Member States where the controller or processor has an establishment on the territory of their Member State, where data subjects on their territory are substantially affected, or where a complaint has been lodged with them. Also where a data subject not situated in that Member State has lodged a complaint, the supervisory authority to which such complaint has been lodged should also be a concerned supervisory authority. Within its tasks to issue guidelines on any question covering the application of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned

			objection.
			(102b) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the concerned supervisory authorities in the decision-making process. If a concerned authority objects to the draft decision proposed by the lead authority, the matter shall be referred to the consistency mechanism as described in Article 57. In cases where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority at which the complaint has been lodged.
			(102c) The decision should be agreed jointly by the lead supervisory authority and the concerned supervisory authorities and should be directed towards the main or single establishment of the

			controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure the compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.
(103) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.	(103) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.	(103) The supervisory authorities should assist each other in performing their ~~duties~~ ***tasks*** and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. ***Where a supervisory authority requesting mutual assistance, in the case of no response of the requested supervisory authority within one month of receiving the request, adopts a provisional measure, such provisional measure should be duly justified and only of a temporary nature.***	(103) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.

(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.	(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.	(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.	(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The European Data Protection Board should be in charge of elaborating the principles regulating the practical aspects for such cooperation.
	Amendment 71		
(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, , or to the monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission	(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring ***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	(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~~ ***adopt*** a measure ***intended to produce legal effects*** as regards processing operations ~~that are related to the offering of goods or services to data subjects in several Member States, , or to the monitoring such data subjects, or that might~~ ***which*** substantially affect ***a significant number of data subjects in several Member States.***	(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities should be established. The Board should issue an opinion in the cases defined by the Regulation but also at the request of one of its members for a matter of general application regarding a processing having effect in at least two Member States. In case a supervisory authority does not intend to follow the opinion of the Board, the latter can adopt a decision that will be binding upon the supervisory authority concerned.

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.	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.	~~the free flow of personal data.~~ It should also apply where any ***concerned*** supervisory authority or the Commission requests that ~~the~~ ***such*** 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.	
(106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a simple majority of its members so decides or if so requested by any supervisory authority or the Commission.	(106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a simple majority of its members so decides or if so requested by any supervisory authority or the Commission.	(106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a ~~simple~~ majority of its members so decides or if so requested by any ***concerned*** supervisory authority ***concerned*** or the Commission. ***The European Data Protection Board should also be empowered to adopt legally binding decisions in case of disputes between supervisory authorities. For that purposes it should issue, in principle with a two-third majority of its members, legally binding decisions in clearly defined cases where there are conflicting views among***	(106) The Board shall also issue binding decisions when a concerned authority has expressed an objection to a draft decision of the lead authority or the lead authority has rejected an objection, or to designate the lead authority when there is no consensus on this issue, or when the competent authority does not intend to follow the opinion issued by the Board in accordance with Article 58(1). The decision shall be adopted by a majority of two-thirds of the members of the Board.

		supervisory authorities in particular in the cooperation mechanism between the lead supervisory authority and concerned supervisory authorities on the merits of the case, notably whether there is an infringement of this Regulation or not.	
	Amendment 72		
	(106a) In order to ensure the consistent application of this Regulation, the European Data Protection Board may in individual cases adopt a decision which is binding on the competent supervisory authorities.		
	Amendment 73		
(107) In order to ensure compliance with this Regulation, the Commission may adopt an opinion on this matter, or a decision, requiring the supervisory authority to suspend its draft measure.	***deleted***	***deleted***	

(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 supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.	(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 supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.	(108) There may be an urgent need to act in order to protect the ***rights and freedoms*** ~~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 period of validity when applying the consistency mechanism.	(108) There may be an urgent need to act in order to protect the rights and freedoms 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 period of validity when applying the consistency mechanism.
(109) 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.	(109) 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.	(109) The application of this mechanism should be a condition for the ~~legal validity and enforcement of the respective decision~~ ***lawfulness of a measure intended to produce legal effects*** by a supervisory authority ***in those cases where its application is mandatory***. In other cases of cross-border relevance, ***the co-operation mechanism between the lead supervisory authority and concerned supervisory authorities should be applied and*** mutual assistance and joint ~~investigations~~ ***operations*** might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering	(109) The application of the consistency mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority.

		the consistency mechanism.	
	Amendment 74		
(110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.	(110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. ~~The Commission should participate in its activities.~~ The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the ~~Commission~~ ***institutions of the Union*** and promoting co-operation of the supervisory authorities throughout the Union***, including the coordination of joint operations***. The European Data Protection Board should act independently when exercising its tasks. ***The European Data Protection Board should strengthen the dialogue with concerned stakeholders such as***	(110) ***In order to promote the consistent application of this Regulation,*** ~~At Union level, a~~ ***the*** European Data Protection Board should be set up ***as an independent body of the Union***. ***To fulfil its objectives, the European Data Protection Board should have legal personality. The European Data Protection Board should be represented by its Chair.*** It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State ***or his or her representative*** ~~and of~~***.*** ~~the~~ ***The Commission and the*** European Data Protection Supervisor~~. The Commission~~ should participate in its activities ***without voting rights***. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission***, in***	(110) In order to promote the consistent application of this Regulation at Union level, the European Data Protection Board should be set up as an independent body of the Union. To fulfil its objectives, the European Data Protection Board should have legal personality. The European Data Protection Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor, or his or her representative. The Commission should participate in its activities. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries

	data subjects' associations, consumer organisations, data controllers and other relevant stakeholders and experts.	***particular on the level of protection in third countries or international organisations,*** and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.	or international organisations, and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.
		(110a) The European Data Protection Board should be assisted by a secretariat provided by the secretariat of the European Data Protection Supervisor. The staff of the secretariat of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation should perform its tasks exclusively under the instructions of, and report to the Chair of the European Data Protection Board. Organisational separation of staff should concern all services needed for the independent functioning of the European Data Protection Board.	(110a) The European Data Protection Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the European Data Protection Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the European Data Protection Board. Organisational separation should concern services needed for the independent functioning of the European Data Protection Board. The European Data Protection Board and the European Data Protection Supervisor shall establish a Memorandum of Understanding implementing such organisational

			arrangements.
	Amendment 75		
(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.	(111) ~~Every data~~ ***Data*** ~~subject~~ ***subjects*** should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to ~~a~~ ***an effective*** judicial remedy ***in accordance with Article 47 of the Charter*** ~~***of Fundamental Rights***~~ 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.	(111) Every data subject should have the right to lodge a complaint with a supervisory authority***, in particular in the Member State of his or her habitual residence,*** ~~in any Member State~~ and have the right to a***n effective*** judicial remedy ***in accordance with Article 47 of the Charter of Fundamental Rights if the data subject*** ~~if they~~ considers that ~~their~~ ***his or her*** rights under this Regulation are infringed or where the supervisory authority does not ~~re~~act on a complaint***, partially or wholly rejects or dismisses a complaint*** or does not act where such action is necessary to protect the rights of the data subject. ***The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with***	(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 an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights of the European Union 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. All complaints must be handled with due diligence, in accordance with this Regulation.

		another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.	
	Amendment 76		
(112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.	(112) Any body, organisation or association which ~~aims to protects the rights and interests of data subjects in relation to the protection of their data~~ ***acts in the public interest*** and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority ***on behalf of data subjects with their consent*** or exercise the right to a judicial remedy ~~on behalf of~~ ***if mandated by the*** data ~~subjects~~***subject***, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a ~~personal data~~ breach ***of this Regulation*** has	(112) ***Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a***~~Any~~ body, organisation or association which aims to protect~~s~~ the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State~~, should have the right~~ to lodge a complaint ***on his or her behalf*** with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects***. Member States may provide that such a body, organisation or association should have the right***~~, or~~ to lodge,	(112) Any body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, a documented claim where it considers that a breach of this Regulation has occurred.

	occurred.	independently of a data subject's ***mandate, in such Member State a*** complaint, ***and/or have the right to*** an ~~own~~ ***effective judicial remedy*** ~~complaint~~ where it ***has reasons to*** considers that ***the rights of a data subject have been infringed as a result of the processing of*** ~~a~~ personal data ~~breach has occurred~~ ***which is not in compliance with this Regulation. This body, organisation or association may not be allowed to claim compensation on a data subject's behalf***.	

(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.	(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.	(113) ~~Each~~ ***Any*** natural or legal person ~~should have~~ ***has*** the right to ***bring*** a***n action for annulment of decisions of the European Data Protection Board before the Court of Justice of the European Union (the "Court of Justice") under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the concerned supervisory authorities who wish to challenge them, have to bring action within two months of their notification to them, in accordance with Article 263 TFEU. Where decisions of the European Data Protection Board are of direct and individual concern to a controller, processor or the complainant, the latter may bring an action for annulment against those decisions and they should do so within two months of their publication on the website of the European Data Protection Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective*** judicial remedy ***before the competent national court*** against ***a*** decision~~s~~ of a supervisory authority	(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.

		which produces legal effects concerning ~~them~~***this person***. ***Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority.*** Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established ***and should be conducted in accordance with the national procedural law of that Member State. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings to the courts in the same Member State. In the***	

		context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the European Data Protection Board is challenged before a national court and the validity of the decision of the European Data Protection Board is at issue, that national court does not have the power to declare the European Data Protection Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice in the Foto-frost case[7] , whenever it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the	

[7] Case C-314/85

		European Data Protection Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down by Article 263 TFEU.	

		(113a) Where a court seized with a proceeding against a decision of a supervisory authority has reason to believe that proceedings concerning the same processing such as the same subject matter as regards processing of the same controller or processor activities or the same cause of action are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if the latter has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.	

	Amendment 77		
(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of data subjects in relation to the protection of their data to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.	(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may ~~request~~ ***mandate*** any body, organisation or association ~~aiming to protect the rights and interests of data subjects in relation to the protection of their data~~ ***acting in the public interest*** to bring ~~on the data subject's behalf~~ proceedings against that supervisory authority to the competent court in the other Member State.	***deleted***	

	Amendment 78		
(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.	(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. ***This does not apply to non-EU residents.*** The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.	***deleted***	

	Amendment 79		
(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority acting in the exercise of its public powers.	(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or***, in case of EU residence,*** where the data subject resides, unless the controller is a public authority ***of the Union or a Member State*** acting in the exercise of its public powers.	(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority acting in the exercise of its public powers.	(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.
(117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.	(117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.	***deleted***	

	Amendment 80		
(118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure.	(118) Any damage***, whether pecuniary or not,*** which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability ***only*** if ~~they prove~~ ***he proves*** that ~~they are~~ ***he is*** not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure.	(118) Any damage which a person may suffer as a result of ~~unlawful~~ processing ***that is not in compliance with this Regulation*** should be compensated by the controller or processor, who ~~may~~ ***should*** be exempted from liability if they prove that they are not ***in any way*** responsible for the damage~~, in particular where he establishes fault on the part of the data subject or in case of force majeure~~. ***The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law.*** ***When reference is made to a processing that is not in compliance with this Regulation it***	(118) Any material or immaterial damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the event giving raise to the damage. Data subjects should receive full and effective compensation for the damage they have suffered.

		also covers processing that is not in compliance with delegated and implementing acts adopted in accordance with this Regulation and national law specifying rules of this Regulation. ***Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with national law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor who has paid full compensation, may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.***	

		(118a) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 should not prejudice the application of such specific rules.	
		(118b) In order to strengthen the enforcement of the rules of this Regulation, penalties and administrative fines may be imposed for any infringement of the Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of	

		the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor.	
		The imposition of penalties and administrative fines should be subject to adequate procedural safeguards in conformity with general principles of Union law and the Charter of Fundamental Rights, including effective judicial protection and due process. Where the national law of a Member State does not provide for administrative fines, such Member State may abstain from providing administrative fines for infringements of this Regulation that are already subject to criminal	

		sanctions in their national law ensuring that these criminal sanctions are effective, proportionate and dissuasive, taking into account the level of administrative fines provided for in this Regulation.	
	Amendment 81		
(119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.	(119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties. ***The rules on penalties should be subject to appropriate procedural safeguards in conformity with the general principles of Union law and the Charter ~~of Fundamental Rights~~, including those concerning the right to an effective judicial remedy, due process and the principle of ne bis in idem.***	(119) ***Member States may lay down the rules on criminal sanctions for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of*** ~~Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with~~ this Regulation. ***These criminal sanctions may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal sanctions for infringements of such national rules and of administrative sanctions*** ~~Member States should ensure that the penalties~~ should ~~be effective, proportionate and dissuasive and should take all measures to implement the~~	(119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.

		~~penalties.~~***not lead to the breach of the principle of ne bis in idem, as interpreted by the Court of Justice.***	

			(119ab) Member States may lay down the rules on criminal sanctions for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. These criminal sanctions may also allow for the deprivation of the profits obtained through infringements of this Regulation.
	Amendment 82		
	(119a) In applying penalties, Member States should show full respect for appropriate procedural safeguards, including the right to an effective judicial remedy, due process, and the principle of ne bis in idem.		(119a) In applying penalties, including criminal sanctions, Member States should show full respect for appropriate procedural safeguards, including the right to an effective judicial remedy, due process, and the principle of *ne bis in idem*.
(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each	(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each	(120) In order to strengthen and harmonise administrative ~~sanctions~~ ***penalties*** against infringements of this Regulation, each supervisory authority should have the power to ***impose*** ~~sanction~~ administrative ~~offences~~***fines***. This Regulation should indicate ~~these~~ offences~~and~~***,*** the upper limit ***and criteria*** for ***fixing*** the related administrative	(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each

individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.	individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.	fines, which should be ~~fixed~~ ***determined by the competent supervisory authority*** in each individual case***, taking into account all relevant circumstances of*** ~~proportionate to~~ the specific situation, with due regard in particular to the nature, gravity and duration of the breach ***and of its consequences and the measures taken to ensure compliance with the obligations under the Regulation and to prevent or mitigate the consequences of the infringement***. ***Where the fines are imposed on persons that are not a commercial undertaking, the supervisory authority should take account of the general level of income in the Member State in considering the appropriate amount of fine.*** The consistency mechanism may also be used to ***promote a consistent*** ~~cover divergences in the~~ application of administrative ~~sanctions~~***fines***. ***It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of***	individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. Where the fines are imposed on persons that are not a commercial undertaking, the supervisory authority should take account of the general level of income in the Member State in considering the appropriate amount of fine. It should be for the Member States to determine whether and to which extent public authorities should be subject to pecuniary fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other sanctions under the Regulation. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.

		the supervisory authorities or of other sanctions under the Regulation.	

		(120a) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of the Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties (criminal or administrative) should be determined by national law.	
	Amendment 83		
(121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of	(121) ~~The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption~~ ***Whenever necessary, exemptions or derogations*** from the requirements of certain provisions of this Regulation ***for the processing of personal data should be provided for*** in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the	(121) ***Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation.*** The processing of personal data solely for journalistic purposes, or for the purposes of ***academic,*** artistic or literary expression should ***be subject to*** ~~qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the~~	(121) Whenever necessary, exemptions or derogations from the requirements of certain provisions of this Regulation for the processing of personal data should be provided for in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. Therefore, Member States should adopt legislative measures, which should

personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as 'journalistic' for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure	Charter~~of Fundamental Rights of the European Union~~. ~~This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries.~~ Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities~~,~~ ~~and~~ on co-operation and consistency ***and on specific data processing situations***. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom~~,~~ ~~such as journalism,~~ broadly~~.~~ ~~Therefore, Member States should classify activities as "journalistic"~~	~~protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union.~~ ***derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data, with the right to freedom of expression and information, as guaranteed by Article 11 of the Charter of Fundamental Rights of the European Union.*** This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities	lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations may relate to general principles, to the rights of the data subject, to controller and processor, to the transfer of data to third countries or international organisations, to the independent supervisory authorities, and to co-operation and consistency and to specific data processing situations. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom broadly to cover all activities which aim at the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them, also taking into account technological development. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making

to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.	~~for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these~~ ***to cover all*** activities ~~is~~ ***which aim at*** the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them***, also taking into account technological development***. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.	and on co-operation and consistency. ***In case these exemptions or derogations differ from one Member State to another, the national law of the Member State to which the controller is subject should apply.*** ~~This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as 'journalistic' for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.~~***In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary***	purposes.

		to interpret notions relating to that freedom, such as journalism, broadly.	
		(121a) **This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Public access to official documents may be considered as a public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by this authority or body if the disclosure is provided for by Union law or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary derogations from the rules of this regulation. The reference to public authorities and bodies should in this context include all authorities or other bodies covered by Member State law on**	(121a) Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation. Personal data in public sector information held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject. However, such obligations, including those set forth in Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information leave intact and in no

		public access to documents. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data.	way prejudice the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular do not alter the obligations and rights set out in this Regulation.
(122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be	(122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be	***deleted***	

justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.	justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.		

	Amendment 84		
	(122a) A professional who processes personal data concerning health should receive, if possible, anonymised or pseudonymised data, leaving the knowledge of the identity only to the ~~General~~ general ~~Practitioner~~ practitioner or to the ~~Specialist~~ specialist who has requested such data processing.		
	Amendment 85		
(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs,	(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council[1] ~~of 16 December 2008 on Community statistics on public health and health and safety at work~~, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs,	***deleted***	(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008*, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the

resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.	resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. ~~Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.~~ _____ ***[1b] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).***		causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies. _____ ** Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).*

	Amendment 86		
	123a) The processing of personal data concerning health, as a special category of data, may be necessary for reasons of historical, statistical or scientific research. Therefore this Regulation foresees an exemption from the requirement of consent in cases of research that serves a high public interest.		
	Amendment 87		
(124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the processing of personal data in the employment sector.	(124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment ***and the social security*** context. ~~Therefore, in order~~ ***Member States should be able*** to regulate the processing of employees' personal data in the employment ***and the processing of personal data in the social security*** context ***in accordance with the rules and minimum standards set out in***~~, Member States should be able, within the limits of~~ this Regulation~~, to adopt by law specific rules for~~***. Where a statutory basis is provided in the Member State in***	(124) ~~The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the processing of personal data in the employment sector.~~ ***National law or collective agreements (including 'works agreements') may provide for*** **specific rules on the processing of employees' personal data in the employment context,**	(124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. Member States should be able to regulate the processing of employees' personal data in the employment context within the limits of this Regulation. Where a statutory basis is provided in the Member State in question for the regulation of employment matters by collective agreement or under Directive 2009/38/EC of the European Parliament and of the Council*, the processing of personal data in an employment context may also be regulated by

	question for the regulation of employment matters by agreement between employee representatives and the management of the undertaking or the controlling undertaking of a group of undertakings (collective agreement) or under Directive 2009/38/EC of the European Parliament and of the Council[1], the processing of personal data in ~~the~~ ***an*** employment ~~sector~~ ***context may also be regulated by such an agreement.*** _____ ***[1] Directive 2009/38/EC of the European Parliament and of the Council of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees (OJ L 122, 16.5.2009, p. 28).***	**in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace , health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.**	such an agreement. _____ ** Directive 2009/38/EC of the European Parliament and of the Council of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees (OJ L 122, 16.5.2009, p. 28).*

(125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.	(125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.	(125) The processing of personal data for the purposes of historical, statistical or scientific ~~research~~ ***purposes and for archiving purposes in the public interest*** should, ***in addition to the general principles and specific rules of this Regulation, in particular as regards the conditions for*** ~~in order to be~~ lawful ***processing***, also ***comply with*** respect to other relevant legislation such as on clinical trials. ***The further processing of personal data for historical, statistical and scientific purposes and for archiving purposes in the public interest should not be considered incompatible with the purposes for which the data are initially collected and may be processed for those purposes for a longer period than necessary for that initial purpose. Member States should be authorised to provide, under specific conditions and in the presence of appropriate safeguards for data subjects, specifications and derogations to the information requirements and the rights to***	(125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.

		access, rectification, erasure, to be forgotten, restriction of processing and on the right to data portability and the right to object when processing personal data for historical, statistical or scientific purposes and for archiving purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles.	

	Amendment 88		
	(125a) Personal data may also be processed subsequently by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest. Member State legislation should reconcile the right to the protection of personal data with the rules on archives and on public access to administrative information. Member States should encourage the drafting, in particular by the European Archives Group, of rules to guarantee the confidentiality of data vis-à-vis third parties and the authenticity, integrity and proper conservation of data.		

		(125aa) By coupling information from registries, researchers can obtain new knowledge of great value when it comes to e.g. widespread diseases as cardiovascular disease, cancer, depression etc. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about long-term impact of a number of social conditions e.g. unemployment, education, and the coupling of this information to other life conditions. Research results obtained on the basis of registries provide solid, high quality knowledge, which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people, and improve the efficiency of social services etc. ***In order to facilitate scientific research, personal data can be processed for scientific purposes subject to appropriate conditions***	

		and safeguards set out in Member State or Union law. Hence consent from the data subject should not be necessary for each further processing for scientific purposes.	
		(125b) 'The importance of archives for the understanding of the history and culture of Europe' and 'that well-kept and accessible archives contribute to the democratic function of our societies', were underlined by Council Resolution of 6 May 2003 on archives in the Member States[8]. Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. ***Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to***	(125b) For the purposes of this Regulation, public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Where personal data are processed for archiving purposes, this Regulation should also apply to that processing.

[8] OJ C 113, 13.5.2003, p.2.

		records of enduring value for general public interest. Member States should also be authorised to provide that personal data may be further processed for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes.	

	Amendment 89		
(126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area.	(126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. ***The processing of personal data for historical, statistical and scientific research purposes should not result in personal data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.***	(126) ***Where personal data are processed for*** ~~S~~scientific ~~research for the~~ purposes**,** ~~of~~ this Regulation should ***also apply to that processing. For the purposes of this Regulation, processing of personal data for scientific purposes should*** include fundamental research, applied research, ~~and~~ privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area***. Scientific purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific purposes specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data***	(126) Scientific research for the purposes of this Regulation should include both fundamental and applied research, irrespective of whether it is funded publicly or privately. In addition, it should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area.

		subject, the general rules of this Regulation should apply in view of those measures.	
		(126a) Where personal data are processed for historical purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.	
		(126b) For the purpose of consenting to the participation in scientific research activities in clinical trials the relevant provisions of Regulation (EU) No. 536/2014 of the European Parliament and of the Council should apply.	

		(126c) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. **Union law or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for guaranteeing statistical confidentiality.**	
		(126d) **The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in conformity with the statistical principles as set out in Article 338(2) of the Treaty of the Functioning of the European Union, while national statistics should also comply with national law.**	

		Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities provides further specifications on statistical confidentiality for European statistics.	

(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.	(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.	(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. ***This is without prejudice to existing Member State obligations to adopt professional secrecy where required by Union law.***	(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.

	Amendment 90		
(128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation. Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.	(128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, ~~comprehensive~~ ***adequate*** rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation ***and recognised as compliant***. ~~Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.~~ .	(128) This Regulation respects and does not prejudice the status under ***existing constitutional*** ~~national~~ law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. ~~As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation. Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.~~	

	Amendment 91		
(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and	(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of ~~lawfulness of processing~~; specifying ~~the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access~~ ***conditions of icon-based mode for provision of information***; the right to ~~be forgotten and to~~ erasure; ~~measures based on profiling; criteria and~~	(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of ~~lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and~~	

to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory	~~requirements in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer;~~ ***declaring that*** codes of conduct ***are in line with this Regulation***; criteria and requirements for certification mechanisms; ***the adequate level of protection afforded by a third country or an international organisation;*** criteria and requirements for transfers by way of binding corporate rules; ~~transfer derogations;~~ administrative sanctions; processing for health purposes~~;~~ ***and*** processing in the	~~to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct;~~ criteria and requirements for certification mechanisms; ~~criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes.~~ It is of particular importance that the Commission carry out appropriate consultations during its preparatory	

work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.	employment context ~~and processing for historical, statistical and scientific research purposes~~. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, ***in particular with the European Data Protection Board***. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and ***to the*** Council.	work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.	

	Amendment 92		
(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards	(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms ***for specific methods to obtain verifiable consent*** in relation to the processing of personal data of a child; standard ~~procedures and~~ forms for ~~exercising the rights of~~ ***the communication to the*** data subjects ***on the exercise of their*** rights; standard forms for the information to the data subject; standard forms ~~and procedures~~ in relation to the right of access ***including for communicating the personal data to the data subject***; ~~the right to data portability;~~ standard forms in relation to ~~the responsibility of the controller to data protection by design and by default and to~~ the documentation ***to be kept by the controller and the processor***; ~~specific requirements for the security of processing;~~ the standard ~~format and the procedures~~ ***form*** for the notification of a personal data breach to the supervisory authority and ~~the~~	(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: ***standard contractual clauses between controllers and processors and between processors, codes of conduct*** ~~specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact~~	(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: the adequate level of protection afforded by a third country, or one or more territories or specified sectors within that third country or an international organisation, or the lack thereof; and formats and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers*. _____ ** Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying*

and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers45. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.	~~communication of a personal data breach to the data subject~~ ***for documenting a personal data breach***~~; standards and procedures for a data protection impact assessment;~~ forms ~~and procedures~~ for prior ~~authorisation and prior~~ consultation~~; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism~~ ***and information to the supervisory authority***. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[1] ~~of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers~~ In this context, the Commission should consider specific measures for micro, small and medium-sized	~~assessment; forms and procedures for prior authorisation and prior consultation;~~ technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; ***adopt standard data protection clauses; formats and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules***~~disclosures not authorized by Union law~~; mutual assistance; ~~joint operations; decisions under the consistency mechanism~~ ***the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board***. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of	*down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13.*

	enterprises. _____ [1] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by ~~the~~ Member States of the Commission's exercise of implementing powers ***(***OJ L 55, 28.2.2011, p. 13***)***.	implementing powers[9]**.** In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.	

[9] ***Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13.***

	Amendment 93		
(131)The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;, the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a	(131) The examination procedure should be used for the adoption of specifying standard forms ~~in relation to the~~***: for specific methods to obtain verifiable*** consent ***in relation to the processing of personal data*** of a child; ~~standard procedures and forms~~ for ~~exercising the~~ ***the communication to the data subjects on the exercise of their*** rights ~~of data subjects~~; ~~standard forms~~ for the information to the data subject; ~~standard forms and procedures~~ in relation to the right of access ***including for communicating the personal data to the data subject***; ~~the right to data portability;~~ ~~standard forms~~ in relation to the ~~responsibility of~~ ***documentation to be kept by*** the controller ~~to data protection by design and by default and to the documentation~~ ***and the processor***; ~~specific requirements for the security of processing; the standard format and the procedures~~ for the notification of a personal data breach to the supervisory authority and ~~the communication of~~ ***for documenting*** a personal data	(131) The examination procedure should be used for the adoption of ~~specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;, the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation~~ ***implementing acts on standard contractual clauses between controllers and processors and between processors; codes of***	(131) The examination procedure should be used for the adequate level of protection afforded by a third country, or one or more territories or specified sectors within that third country or an international organisation, or the lack thereof; and formats and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules, given that those acts are of general scope.

territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.	breach ~~to the data subject~~; ~~standards and procedures~~ ~~for a data protection impact assessment; forms and procedures~~ for prior ~~authorisation and prior~~ consultation~~; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism~~, ***and information to the supervisory authority,*** given that those acts are of general scope.	***conduct***; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; ~~disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism,~~ ***adopt standard data protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board*** given that those acts are of general scope.	

	Amendment 94		
(132) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.	***deleted***	(132) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection ~~and relating to matters communicated by supervisory authorities under the consistency mechanism~~, imperative grounds of urgency so require.	(132) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country, or one or more territories or specified sectors within that third country or an international organisation which does not ensure an adequate level of protection, imperative grounds of urgency so require.
(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that	(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States ~~and~~ ***but*** can ~~therefore~~***rather***, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that	(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this	(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this

Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	Regulation does not go beyond what is necessary in order to achieve that objective.	Regulation does not go beyond what is necessary in order to achieve that objective.
	Amendment 95		
(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force.	(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force. ***Commission decisions and authorisations by supervisory authorities relating to transfers of personal data to third countries pursuant to Article 41(8) should remain in force for a transition period of five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period.***	(134) Directive 95/46/EC should be repealed by this Regulation. ***Processing already under way on the date of the entry into force of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force***. However, ~~Commission decisions adopted and authorisations by supervisory authorities based on~~ ***where such processing is in compliance with Directive 95/46/EC, the requirements of this Regulation concerning the carrying out of data protection impact assessments and the prior consultation of the supervisory authority should not apply to the processing operations already under way prior to the entry into force of this Regulation, given that these requirements, by their very nature, are to be met prior to the processing. Where such processing is in compliance with*** Directive	(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force until they are amended, replaced or repealed in accordance with this Regulation.

		95/46/EC***, it is also not necessary for the data subject to give his or her consent again so as to allow the controller to continue such processing after the data of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*** ~~should remain in force~~.	

(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.	(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC ***of the European Parliament and of the Council***[1], including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly. [1] ***Directive 2202/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.07.2002, P.37)***	(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly. ***Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.***	(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC on privacy and electronic communications*, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly. _____ ** Directive 2202/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.07.2002, P.37)*

			(135a) In order to enhance the consistency of the regulatory framework for data protection at EU level, the Commission should present, without delay, a proposal aligning Regulation (EC) 45/2001* applicable to the processing of personal data by the Union institutions, bodies, offices and agencies with the principles of the present Regulation, taking into account the specific characteristics of the EU public sector. _____ ** Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1.*

(136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[46]. _____ [46] OJ L 176, 10.7.1999, p. 36.	(136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen ***acquis*** to the extent that it applies to the processing of personal data by authorities involved in the implementation of that ***acquis***, ***within the meaning of*** ~~as provided for by~~ the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the ***latters'*** association ~~of those two States~~ with the implementation, application and development of the Schengen acquis[1]. _____ [1] OJ L 176, 10.7.1999, p. 36.	***deleted***	(136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis*. _____ ** OJ L 176, 10.7.1999, p. 36.*

(137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[47]. _____ [47] OJ L 53, 27.2.2008, p. 52	(137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen ***acquis*** to the extent that it applies to the processing of personal data by authorities involved in the implementation of that ***acquis***, ***within the meaning of*** ~~as provided for by~~ the Agreement between the European Union, the European Community and the Swiss Confederation ~~concerning~~ ***on*** ~~the association of~~ the Swiss Confederation'***s association*** with the implementation, application and development of the Schengen ***acquis***[1]. _____ [1] OJ L 53, 27.2.2008, p. 52	***deleted***	(137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis*. _____ * *OJ L 53, 27.2.2008, p. 52*

(138) As regards Liechtenstein, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[48]. _____ **48** OJ L 160 of 18.6.2011, p. 19	(138) As regards Liechtenstein, this Regulation constitutes a development of provisions of the Schengen ***acquis*** to the extent that it applies to the processing of personal data by authorities involved in the implementation of that ***acquis***, ***within the meaning of*** ~~as provided for by~~ the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen ***acquis***[1]. _____ **1** OJ L 160 of 18.6.2011, p. 19	***deleted***	(138) As regards Liechtenstein, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis*. _____ * *OJ L 160 of 18.6.2011, p. 19*

(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.	(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter ~~of Fundamental Rights of the European Union~~ as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity~~.business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity~~	***deleted***	