Council of the European Union

Brussels, 16 November 2015
(OR. en)

14076/15

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 200
JAI 852
MI 722
DIGIT 91
DAPIX 208
FREMP 260
COMIX 582
CODEC 1512

PUBLIC

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	10391/15, 13914/15
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (first reading) - Preparation of trilogue - Chapters II, III, IV and V

Delegations will find in Annex a comparative table which compares in 4 columns the Commission proposal, the position of the European Parliament in 1st reading, the Council's General Approach and compromises tentatively agreed at previous trilogues as well as compromise suggestions by the Presidency. Text marked in brackets will be discussed by the Permanent Representatives Committee at a later stage in relation to other provisions of the text.

COM (2012)0011	EP Position / First Reading	Council General Approach (15/06/2015)	Tentative agreement in trilogue
(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.	*Tentative agreement in trilogue:* (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.

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 generally used in the third country where the controller is established,***	*Tentative agreement in trilogue:* (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 who are in the Union by a controller or a processor 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 irrespective of whether connected to a payment or not. In order to determine whether such a controller or processor is offering goods or services to data subjects who are 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. 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 generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors

		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.	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 who are in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union.
(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	(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	*Tentative agreement in trilogue:* (21) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects as far as their behaviour takes places 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 including potential subsequent use of data processing techniques which consist of

	him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	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.
(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.	*Tentative agreement in trilogue:* (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.
		(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) (…)***	*Presidency suggestion:* (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.

		(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.	*Presidency suggestion:* (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 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 disruptive to the use of the service for which it is provided.	(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 request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	(25) Consent should be given ~~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 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***	*Presidency suggestion:* (25) Consent should be given 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 statement or, if required by specific circumstances, by any other clear affirmative action by the data subject, signifying his or her agreement to personal data relating to him or her being processed. This 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 their personal data. Silence or inactivity should therefore not constitute consent. 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. In such cases it is sufficient that the data subject receives the information needed to give freely

		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.	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.

		(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.	*Presidency suggestion:* (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.

(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 ~~e.g.~~ ***for example*** from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	*Tentative agreement in trilogue:* (26) Personal data concerning health should include 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 status of the data subject; including information about the individual collected in the course of the registration for and the provision of health care services as referred to in Directive 2011/24/EU to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; 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.

(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".***	*Tentative agreement in trilogue:* (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".

(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.***	*Presidency suggestion:* (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. 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.

(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.	(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.	(30) Any processing of personal data should be lawful ***and***~~,~~ fair**.** ~~and~~ ***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***	*Presidency proposals:* (30) Any processing of personal data should be lawful and fair. It should be transparent for the individuals 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 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

		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 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***	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 limited to what is necessary 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

		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.***	taken to ensure that personal data which are inaccurate are rectified or deleted. 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***.	*Presidency suggestion:* (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.

	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.***	*Presidency suggestion:* (32) Where processing is based on the data subject's consent, the controller should 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 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.

	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 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.***	***(33) deleted***	

	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 deemed as freely given, taking into account the interest of the data subject.	***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 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***	*Presidency suggestion:* (34) In order to safeguard that 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 makes it unlikely that consent was given freely 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.

		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.	
(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.	*Tentative agreement in trilogue:* (35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

(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.***	*Tentative agreement in trilogue:* (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. Personal data should be processed based on the vital interest of another natural person in principle where the processing cannot be manifestly based on another legal basis. 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.

	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 be obliged to explicitly inform the	(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 account whether***	*Presidency suggestion:* (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, taking into consideration the reasonable expectations of data subjects. Legitimate interest could exist for example when there is a relevant and appropriate relationship 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 reasonably expect at the time and in the context of the collection of the data that processing for this purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed

	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.	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***.~~	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. 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.

		(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.	*Presidency suggestion:* (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, 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	(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 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	(39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the ~~concerned~~ data controller **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	*Presidency suggestion:* (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 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 data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code

communication systems.	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.***	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.***	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 Regulation and in particular the information of the data subject on those other purposes should be ensured.	***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 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***	*Presidency suggestion:* (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 such case no separate legal basis is required other than the one which allowed the collection of the data. If 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 in the public interest, or statistical, scientific or historical purposes should be considered as compatible lawful processing operations.] The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for

		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	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, in particular the reasonable expectations of data subjects based on his/her relationship with the controller 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 further processing operations. Where the data subject has given consent or the processing is based on Union or Member State law 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.***	controller shall be allowed to further process the data irrespective of the compatibility of the purposes. 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 specific requirements for such processing, the general principles and other rules of this Regulation should***	*Presidency suggestion:* (41) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, 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 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

		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.***	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 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.

	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 services, especially in order to	*Presidency suggestion:* (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, in particular processing data in the field of of employment law, 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. This may be done for health purposes, including public health 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 archiving in the public interest or historical, statistical and scientific purposes.] A derogation should also allow

		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.***	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***	*Presidency suggestion:* (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

		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.**	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	*Presidency suggestion:* (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

		such as employers, insurance and banking companies.	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.	*Tentative agreement in trilogue:* (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.	*Tentative agreement in trilogue:* (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 rights.***	*Presidency suggestion:* (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. 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 rights. Identification could 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.

(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 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.	*Presidency suggestion:* (46) The principle of transparency requires that any information addressed to the public or to the data subject should be concise, 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 information and communication, where processing is addressed 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.	*Presidency suggestion:* (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 one month and give reasons where the controller, in case he does not intend to comply with the data subject's request.

	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.	*Presidency suggestion:* (48) The principles of fair and transparent processing require that the data subject should be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to guarantee fair and transparent processing having regard to the specific circumstances and context in which the personal data are processed. 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.

(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.***	*Presidency suggestion:* (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.	*Presidency suggestion:* (50) However, it is not necessary to impose this obligation where the data subject already possesses 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 purposes;] in this regard, the number of data subjects, the age of the data, and any 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.	*Tentatively agreed in trilogue:* (51) A natural person should have the right of access to data which has been collected concerning 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 data processing and what might be, at least when based on profiling, the consequences of such processing.

			Where possible, the controller may provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.
		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. ***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.***	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. 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.	*Presidency suggestion:* (52) The controller should use all reasonable measures to verify the identity of a data subject 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 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	(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,~~	(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***	*Presidency suggestion:* (53) 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 in particular

involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in 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.	~~when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.~~ However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in 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.***	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 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~~	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 exercise this right notwithstanding the fact that he or she is no longer a child. However, the further retention of the data should be lawful where it is necessary, 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.

		~~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.~~	*Presidency suggestion:* (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 the controllers which are processing such data to erase any links to, or copies or replications of that personal data. To ensure the above mentioned information, the controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers, which are processing the data, of the data subject's request.

	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) 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.	*Presidency suggestion:* (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***	*Tentative agreement in trilogue:* (55) To further strengthen the control over their own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, machine-readable and interoperable format and transmit to another controller. This right should apply where the data subject provided the personal data based on his or her consent or is necessary for the performance of a contract. It should not apply where processing is based on another legal ground other than consent or 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

		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***	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 receive personal data concerning him or her 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 receive 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

		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.	necessary for the performance of that contract. Where technically feasible and available, the data may be transmitted from one automated application into another one.

	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.	*Presidency suggestion:* (56) In cases where personal data might lawfully be processed 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 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 their particular situation. It should be for the controller to demonstrate that their compelling legitimate interests 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.	*Presidency suggestion:* (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, at any time and free of charge. This right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

	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***	(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,***	*Presidency suggestion:* (58) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing, which produces legal effects concerning him or her or similarly 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 similarly significantly affects him or her. However, decision making based on such processing, including profiling, should be

	union membership, sexual orientation or gender identity.	***should be allowed when expressly authorised 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***	allowed when expressly authorised 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 conducted in accordance with the regulations, standards and recommendations of EU institutions or national oversight bodies 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

		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.	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.	*Presidency suggestion:* (58a) Profiling as such is subject to the 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.

(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.***	*Tentative agreement in trilogue:* (60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation. These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals.

		(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	*Presidency suggestion:* (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.	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.**	*Presidency suggestion:* (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,	*Presidency suggestion:* (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.	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 ultimate deployment, use and final***	(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***	*Tentative agreement in trilogue:* (61) The protection of the rights and freedoms of individuals with regard to the processing of personal data require that appropriate technical and organisational measures are taken, to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement 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 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,

	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.***	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.The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

	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.	*Presidency suggestion:* (62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, 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, and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

	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	*Presidency suggestion:* (63) Where a controller not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller should designate a representative, unless the processing is occasional, does not include processing of special categories of data as referred to in Article 9(1) or processing of data relating to criminal convictions and offences referred to in Article 9a, and is unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing or if 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 representative should be explicitly designated by a written mandate of 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.***	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 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	*Presidency suggestion:* (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	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.	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***	

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

	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***	*Presidency suggestion:* (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, such as encryption. These measures should ensure an appropriate level of security including confidentiality, taking into account state of the art and the costs of implementation in relation to the risk and the nature of the personal data to be protected. 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 processed, which may in particular lead to physical, material or moral damage.	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 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	*Presidency suggestion:* (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.	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	(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***	(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***	*Presidency suggestion:* (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 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

achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would	***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, 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	***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 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	of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred and that this breach is likely to result in a risk for the rights and freedoms of the data subject, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay (67a new) The individuals should be notified without undue delay if the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, in order to allow them to take the necessary precautions. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate

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.	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.	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 implement appropriate measures against continuing or similar data breaches may justify a longer delay.	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 need to mitigate an immediate risk of damage 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.

(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.***	*Presidency suggestion:* (68) It must be ascertained whether 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. 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.

		(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.	*Presidency suggestion: deleted*

(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.	(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.	(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.	*Presidency suggestion:* (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.

(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 this Regulation.	(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 this Regulation.	(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 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***	*Presidency suggestion:* (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 obligations should be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of individuals by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in particular, involve using new technologies, or are of a new kind 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.

		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.	*Presidency suggestion:* (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 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***	*Presidency suggestion:* (71) This should in particular apply to large-scale 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 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

		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.**	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~~egulation.		

	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.	*Tentative agreement in trilogue:* (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.	*Presidency suggestion:* (73) 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, Member States may deem it necessary to carry out such assessment prior to the processing activities.
	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	(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	(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~~	*Presidency suggestion:* (74) Where a data protection impact assessment indicates that the processing would, in the absence of envisaged safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of 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, the supervisory authority should be consulted, prior to the start of processing activities. Such high

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.	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.	~~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 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***	risk is likely to result from certain types of data processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the individual. 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.

		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.	*Presidency suggestion:* (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.	*Presidency suggestion:* (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	(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***.	*Tentative agreement in trilogue:* (75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by an enterprise which have core activities that involve processing operations which require regular and systematic monitoring, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. 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.

	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 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***.	*Presidency suggestion:* (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.

		(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.	*Presidency suggestion:* (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.	*Presidency suggestion:* 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, subject to the other provisions of this Regulation, the conditions laid***	*Tentative agreement in trilogue:* (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

		down in Chapter V are complied with by the controller or processor.	transfer may only take place if, 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.***	*Tentative agreement in trilogue:* (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 approriate 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 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.	(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 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.***	(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 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.	*Tentative agreement in trilogue:* (80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a specified sector 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. The Commission may also decide, having given notice and a complete justification to the third country, to revoke such a decision.

(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***	*Presidency suggestion:* (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, 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 essentially equivalent to that guaranteed within the Union, in

		effective data 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.	particular when data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data 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.
		(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	*Tentative agreement in trilogue:* (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

		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.	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.	*Tentative agreement in trilogue:* (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. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. This periodic review should be made in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and the Council as well as other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter

			decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 as established under this Regulation to the European Parliament, and to the Council.

	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***.	*Tentative agreement in trilogue:* (82) The Commission may recognise that a third country, or a territory or a specified sector within a third country, or an international organisation 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.

	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***	*Tentative agreement in trilogue:* (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, Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to intra-EU processing, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation. They should relate in particular to compliance with the general principles relating to personal data

	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.	***relating 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.***	processing, 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, providing for enforceable and effective rights for data subjects. The authorisation of the competent supervisory authority should be obtained when the safeguards are adduced in non legally binding administrative arrangements.

	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.	*Tentative agreement in trilogue:* (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. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

	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.	*Tentative agreement in trilogue:* (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 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	*Tentative agreement in trilogue: subject to alignment with overall agreement on consent:* (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. 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

		persons or if they are to be the recipients.	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 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 data subject's or another person's life, if the data subject is incapable of giving consent. Transferring 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***	(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 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***	*Tentative agreement in trilogue:* (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 exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in case of contact tracing 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

	circumstances of the transfer should be carried out.	***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 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.***	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 of personal data of a data subject who is physically or legally incapable of giving consent, with the view to accomplishing a task incumbent under the Geneva Conventions 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.

(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***	*Tentative agreement in trilogue:* (88) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects , could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller 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. Such transfers should only be possible in residual cases where none of the other grounds for transfer are applicable. [For the purposes of processing for historical, statistical and scientific research purposes, the legitimate

		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.	expectations of society for an increase of knowledge should be taken into consideration]. The controller shall inform the supervisory authority and the data subject about the transfer.

	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 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.	(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*** 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.***	(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 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.	*Tentative agreement in trilogue:* (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 enforceable and effective rights as regards processing of their data in the Union once this data has been transferred so that that they will continue to benefit from fundamental rights and safeguards.

	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 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.	(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 cases where controllers or processors are confronted with***	(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.~~	*Tentative agreement in trilogue:* (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. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. 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

	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.		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.

(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 legislation for the protection of***	*Tentative agreement in trilogue:* (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

		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.	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.

Article 3	*Article 3*	*Article 3*	*Article 3*
Territorial scope	***Territorial scope***	***Territorial scope***	***Territorial scope***
	Amendment 97		
1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union***, whether the processing takes place in the Union or not***.	1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.	*Tentative agreement in trilogue:* 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2.This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:	2. This Regulation applies to the processing of personal data of data subjects ~~residing~~ in the Union by a controller ***or processor*** not established in the Union, where the processing activities are related to:	2.This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:	*Tentative agreement in trilogue:* 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or	(a) the offering of goods or services***, irrespective of whether a payment of the data subject is required,*** to such data subjects in the Union; or	(a) the offering of goods or services***, irrespective of whether a payment by the data subject is required,*** to such data subjects in the Union; or	*Tentative agreement in trilogue:* (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour.	(b) the monitoring of ~~their behaviour~~ ***such data subjects***.	(b) the monitoring of their behaviour ***as far as their behaviour takes place within the European Union***.	*Tentative agreement in trilogue:* (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	*Tentative agreement in trilogue:* 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Article 4	*Article 4*	*Article 4*	*Article 4*
Definitions	***Definitions***	***Definitions***	***Definitions***
	Amendment 98		
For the purposes of this Regulation:	For the purposes of this Regulation:	For the purposes of this Regulation:	*Tentative agreement in trilogue:* For the purposes of this Regulation:
	(2a) 'pseudonymous data' means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution;		*see definition (3b)*
	(2b) 'encrypted data' means personal data, which through technological protection measures is rendered unintelligible to any person who is not authorised to access them;		

	(3a) 'profiling' means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour;		*Tentative agreement in trilogue:* (3a) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
		(3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;	*Tentative agreement in trilogue:* (3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

		(3b) pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.	*Tentative agreement in trilogue:* (3b) pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.
(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	*Tentative agreement in trilogue:* (4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

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

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	*Tentative agreement in trilogue:* (6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
	(7a) 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;		*Tentative agrrement in trilogue:* (7a) 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	(8) 'the data subject's consent' means any freely given**,** specific~~,~~ ***and*** informed ~~and explicit~~ indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	*Presidency suggestion:* (8) 'the data subject's consent' means any freely given**,** specific and informed indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(9) 'personal data breach' means ~~a breach of security leading to~~ the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	*Tentative agreement in trilogue :* (9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means all ***personal*** data~~, of whatever type, concerning~~ ***relating to*** the ***genetic*** characteristics of an individual which ~~are~~ ***have been*** inherited or acquired ~~during early prenatal development~~ ***as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, desoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained;***	(10) 'genetic data' means all ***personal*** data~~, of whatever type, concerning~~ ***relating to the genetic*** characteristics of an individual ~~which are inherited or acquired during early prenatal development~~ ***that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;***	*Tentative agreement in trilogue:* (10) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;	(11) 'biometric data' means any ***personal*** data relating to the physical, physiological or behavioural characteristics of an individual which allow his or her unique identification, such as facial images, or dactyloscopic data;	(11) 'biometric data' means any ***personal*** data ***resulting from specific technical processing*** relating to the physical, physiological or behavioural characteristics of an individual which allow***s or confirms the*** ~~their~~ unique identification ***of that individual***, such as facial images, or dactyloscopic data;	*Tentative agreement in trilogue:* (11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allow***s*** or confirms the unique identification of that individual, such as facial images, or dactyloscopic data;
(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health' means any ~~information~~ ***personal data*** which relate to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health' means ***data related*** ~~any information which relates~~ to the physical or mental health of an individual, ***which reaveal information about his or her health status*** ~~or to the provision of health services to the individual~~;	*Tentative agreement in trilogue:* (12) 'data concerning health' means personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status."
		(12a) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements;	*see definition 3a*

(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;	(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, ~~acts and may be addressed by any supervisory authority and other bodies in the Union instead of~~ ***represents*** the controller, with regard to the obligations of the controller under this Regulation;	(14) 'representative' means any natural or legal person established in the Union who, ~~explicitly~~ designated by the controller ***in writing pursuant to Article 25***, ***represents*** ~~acts and may be addressed by any supervisory authority and other bodies in the Union instead of~~ the controller, with regard to the obligations of the controller under this Regulation;	*Tentative agreement in trilogue:* (14) 'representative' means any natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 25, represents the controller or processor, with regard to their respective obligations under this Regulation;
(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	(15) 'enterprise' means any ***natural or legal person*** ~~entity~~ engaged in an economic activity, irrespective of its legal form, ~~thus~~ including, ~~in particular, natural and legal persons,~~ partnerships or associations regularly engaged in an economic activity;	*Tentative agreement in trilogue:* (15) 'enterprise' means any natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	*Tentative agreement in trilogue:* (16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;	(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;	(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings ***or group of enterprises engaged in a joint economic activity***;	*Tentative agreement in trilogue:* (17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings or group of enterprises engaged in a joint economic activity;
(18) 'child' means any person below the age of 18 years;	(18) 'child' means any person below the age of 18 years;	***deleted***	
		(20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.	*Tentative agreement in trilogue:* (20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.

		(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;	*Tentative agreement in trilogue:* (21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;

CHAPTER II PRINCIPLES	CHAPTER II PRINCIPLES	CHAPTER II PRINCIPLES	CHAPTER II PRINCIPLES
Article 5	***Article 5***	***Article 5***	***Article 5***
Principles relating to personal data processing	***Principles relating to personal data processing***	***Principles relating to personal data processing***	***Principles relating to personal data processing***
	Amendment 99		
Personal data must be:	1. Personal data ~~must~~***shall*** be:	Personal data must be:	*Tentative agreement in trilogue:* 1. Personal data must be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;	(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***(lawfulness, fairness and transparency)***;	(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;	*Tentative agreement in trilogue:* (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;	(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ***(purpose limitation)***;	(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; ***further processing of personal data for archiving purposes in the public interest or scientific, statistical or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes;***	*Tentative agreement in trilogue:* (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; [further processing of personal data for archiving purposes in the public interest or scientific, statistical or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes;] ("purpose limitation")

(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;	(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data ***(data minimisation)***;	(c) adequate, relevant, and ***not excessive*** ~~limited to the minimum necessary~~ in relation to the purposes for which they are processed; ~~they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;~~	*Tentative agreement in trilogue:* (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*data minimisation*);
(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	(d) accurate and***, where necessary,*** kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***(accuracy).***	(d) accurate and***, where necessary,*** kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	*Tentative agreement in trilogue:* (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;	(e) kept in a form which permits ***direct or indirect*** identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research ***or for archive*** purposes in accordance with the rules and conditions of ~~Article~~ Articles 83 ***and 83a*** and if a periodic review is carried out to	(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed ~~solely~~ for ***archiving purposes in the public interest, or*** **scientific**, ~~historical,~~ statistical***,*** ~~or scientific research~~ ***or historical*** purposes in accordance with ~~the rules and conditions of~~ Article 83 ~~and if a periodic review is carried~~	*Presidency suggestion:* (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; [personal data may be stored for longer periods insofar as the data will be processed [solely] for archiving purposes in the public interest, or scientific, statistical, or historical purposes in accordance with

	assess the necessity to continue the storage, ***and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes (storage minimisation)***;	~~out to assess the necessity to continue the storage~~***subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject;***	Article 83 subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject] ("storage limitation");
	(ea) processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness);		
	(eb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity);		*Tentative agreement in trilogue:* (eb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality");
		(ee) processed in a manner that ensures appropriate security of the personal data.	

(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.	(f) processed under the responsibility and liability of the controller, who shall ensure and ***be able to*** demonstrate ~~for each processing operation~~ the compliance with the provisions of this Regulation ***(accountability)***.	***deleted***	
		2. The controller shall be responsible for compliance with paragraph 1.	*Tentative agreement in trilogue:* 2. The controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability").

Article 6	*Article 6*	*Article 6*	*Article 6*
Lawfulness of processing	***Lawfulness of processing***	***Lawfulness of processing***	***Lawfulness of processing***
	Amendment 100		
1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:	*Tentative agreement in trilogue:* 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	(a) the data subject has given ***unambiguous*** consent to the processing of their personal data for one or more specific purposes;	*Presidency suggestion:* (a) the data subject has given unambiguous consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	*Tentative agreement in trilogue:* (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	*Tentative agreement in trilogue:* (c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;	(d) processing is necessary in order to protect the vital interests of the data subject;	(d) processing is necessary in order to protect the vital interests of the data subject ***or of another person***;	*Tentative agreement in trilogue:* (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	*Tentative agreement in trilogue:* (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	(f) processing is necessary for the purposes of the legitimate interests pursued by ***the*** controller ***or***, ***in case of disclosure, by the third party to whom the data ~~is~~ are disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller***, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data~~, in particular where the data subject is a child~~. This shall not apply to processing carried out by public authorities in the performance of their tasks.	(f) processing is necessary for the purposes of the legitimate interests pursued by ~~a~~ ***the*** controller ***or by a third party***, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. ~~This shall not apply to processing carried out by public authorities in the performance ***exercise*** of their tasks.~~	*Presidency suggestion:* (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance exercise of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.	2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.	2. Processing of personal data which is necessary for ***archiving*** ~~the~~purposes ***in the public interest, or*** ~~of~~***for*** historical, statistical or scientific ~~research~~ ***purposes*** shall be lawful subject ***also*** to the conditions and safeguards referred to in Article 83.	*Presidency suggestion:* [2. Processing of personal data which is necessary for archiving purposes in the public interest, or for historical, statistical or scientific purposes shall be lawful subject also to the conditions and safeguards referred to in Article 83.]
[…]	[…]	[…]	[…]

		3a. In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account, unless the data subject has given consent, inter alia:	*Presidency suggestion:* 3a. Where the processing for another purpose than the one for which the data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in points (aa) to (g) of Article 21(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the data are initially collected, take into account, inter alia:
		(a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;	*Presidency suggestion:* (a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;
		(b) the context in which the data have been collected;	*Presidency suggestion:* (b) the context in which the data have been collected, in particular regarding the relationship between data subjects and the controller;

		(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9;	*Presidency suggestion:* (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 or whether data related to criminal convictions and offences are processed, pursuant to Article 9a;
		(d) the possible consequences of the intended further processing for data subjects;	*Presidency suggestion:* (d) the possible consequences of the intended further processing for data subjects;
		(e) the existence of appropriate safeguards.	*Presidency suggestion:* (e) the existence of appropriate safeguards

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.	***deleted***	4. Where the purpose of further processing is ~~not~~ ***in***compatible with the one for which the personal data have been collected ***by the same controller***, the ***further*** processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. ~~This shall in particular apply to any change of terms and general conditions of a contract.~~ ***Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject.***	*Presidency suggestion: deleted*
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.	***deleted***	***deleted***	

Article 7	*Article 7*	*Article 7*	*Article 7*
Conditions for consent	***Conditions for consent***	***Conditions for consent***	***Conditions for consent***
	Amendment 101		
1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.	1. ***Where processing is based on consent,*** ~~T~~***the*** controller shall bear the burden of proof for the data subject's consent to the processing of ~~their~~ ***his or her*** personal data for specified purposes.	1. ***Where Article 6(1)(a) applies*** the controller shall ~~bear the burden of proof for the data subject's~~ ***be able to demonstrate that unambiguous*** consent ~~to the processing of their personal data for specified purposes~~ ***was given by the data subject***.	*Tentative agreement in trilogue:* 1. Where processing is based on consent, the controller shall be able to demonstrate that consent was given by the data subject to the processing of their personal data.
		1a. Where Article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.	
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.	2. If the data subject's consent is given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented ***clearly*** distinguishable in its appearance from this other matter. ***Provisions on the data subject's consent which are partly in violation of this Regulation are fully void.***	2. If the data subject's consent is to be given in the context of a written declaration which also concerns ~~an~~other matter***s***, the ~~requirement to give~~***request for*** consent must be presented ***in a manner which is clearly*** distinguishable ~~in its appearance~~ from th~~is~~***e*** other matter***s, in an intelligible and easily accessible form, using clear and plain language***.	*Presidency suggestion:* 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the requirement for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration which constitutes an infringement of this Regulation

			that the data subject has given consent to shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	3. ***Notwithstanding other legal grounds for processing,*** ~~T~~***the*** data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. ***It shall be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller.***	3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal***. Prior to giving consent, the data subject shall be informed thereof.***	*Tentative agreement in trilogue:* 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal**.** Prior to giving consent, the data subject shall be informed thereof. IT shall be as easy to withdraw consent as to give it.

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	4. Consent shall ~~not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller~~ ***be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b)***.	***deleted***	*Presidency suggestion:* 4. When assessing whether consent is freely given, account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract, where processing is based on Article 6(1)(b).

Article 8	*Article 8*	*Article 8*	*Article 8*
Processing of personal data of a child	***Processing of personal ~~data~~ of a ~~child~~ child***	***Conditions applicable to child's consent in relation to information society services***	***Conditions applicable to child's consent in relation to information society services***
	Amendment 102		
1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.	1. For the purposes of this Regulation, in relation to the offering of ~~information society~~ ***goods or*** services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or ~~custodian~~***legal guardian***. The controller shall make reasonable efforts to ~~obtain verifiable~~ ***verify such*** consent, taking into consideration available technology ***without causing otherwise unnecessary processing of personal data***.	1. ~~For the purposes of this Regulation~~***Where Article 6 (1)(a) applies***, in relation to the offering of information society services directly to a child, the processing of personal data of a child ~~below the age of 13 years~~ shall only be lawful if and to the extent that ***such*** consent is given or authorised by the ***holder of parental responsibility over the*** child~~'s parent~~ or ~~custodian~~***is given by the child in circumstances where it is treated as valid by Union or Member State law***.	*Presidency suggestion:* 1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 16 years shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child.
	1a. Information provided to children, parents and legal guardians in order to express consent, including about the controller's collection and use of personal data, should be given in a clear language appropriate to the intended audience.		

		1a. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	*Tentative agreement in trilogue:* 1a. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	*Tentative agreement in trilogue:* 2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	3. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~ ***entrusted with the task*** of ~~further specifying the criteria and requirements~~ ***issuing guidelines, recommendations and best practices*** for the methods ~~to obtain verifiable~~ ***of verifying*** consent referred to in paragraph 1***, in accordance with Article 66***. ~~In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.~~	***deleted***	

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	
Article 9	***Article 9***	***Article 9***	***Article 9***
	Amendment 103		
Processing of special categories of personal data	~~***Processing of special***~~ ***Special categories of*** ~~**personal**~~ ***data***	***Processing of special categories of personal data***	***Processing of special categories of personal data***
1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.	1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or ***philosophical*** beliefs, ***sexual orientation or gender identity,*** trade-union membership ***and activities***, and the processing of genetic ***or biometric*** data or data concerning health or sex life~~or~~***, administrative sanctions, judgments,*** criminal ***or suspected offences,*** convictions or related security measures shall be prohibited.	1. The processing of personal data, revealing ~~race~~ ***racial*** or ethnic origin, political opinions, religio~~n~~***us*** or ***philosophical*** beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life ~~or criminal convictions or related security measures~~ shall be prohibited.	*Presidency suggestion:* 1. The processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life and sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply where:	2. Paragraph 1 shall not apply~~where~~ ***if one of the following applies:***	2. Paragraph 1 shall not apply ***if one of the following applies:***	*Presidency suggestion:* 2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	(a) the data subject has given consent to the processing of those personal data ***for one or more specified purposes***, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	(a) the data subject has given ***explicit*** consent to the processing of those personal data, ~~subject to the conditions laid down in Articles 7 and 8,~~ except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	*Presidency suggestion:* (a) the data subject has given explicit consent to the processing of those personal, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or
	(aa) processing is necessary for the performance or execution of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;		
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or	(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law ***or collective agreements*** providing for adequate safeguards ***for the fundamental rights and the interests of the data subject such as right to non-discrimination, subject to the conditions and safeguards referred to in Article 82***; or	(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller ***or of the data subject*** in the field of employment ***and social security and social protection*** law in so far as it is authorised by Union law or Member State law ***or a collective agreement pursuant to Member State law*** providing for adequate safeguards; or	*Presidency suggestion:* (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union law or Member State law or a collective agreement pursuant to Member State law providing for adequate safeguards for the fundamental rights and the interests of the data subject; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or	(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or	(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or	*Tentative agreement in trilogue:* (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or	(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or	(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or	*Tentative agreement in trilogue:* (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or
(e) the processing relates to personal data which are manifestly made public by the data subject; or	(e) the processing relates to personal data which are manifestly made public by the data subject; or	(e) the processing relates to personal data which are manifestly made public by the data subject; or	*Tentative agreement in trilogue:* (e) the processing relates to personal data which are manifestly made public by the data subject; or

(f) processing is necessary for the establishment, exercise or defence of legal claims; or	(f) processing is necessary for the establishment, exercise or defence of legal claims; or	(f) processing is necessary for the establishment, exercise or defence of legal claims ***or whenever courts are acting in their judicial capacity***; or	*Tentative agreement in trilogue:* (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or	(g) processing is necessary for the performance of a task carried out ~~in the~~ ***for reasons of high*** public interest, on the basis of Union law, or Member State law which shall ***be proportionate to the aim pursued, respect the essence of the right to data protection and*** provide for suitable measures to safeguard the ***fundamental rights and the*** ~~data subject's legitimate~~ interests ***of the data subject***; or	(g) processing is necessary for ~~the performance of a task carried out in the~~ ***reasons of*** public interest, on the basis of Union law, or Member State law which shall provide for suitable ***and specific*** measures to safeguard the data subject's legitimate interests; or	*Presidency suggestion:* (g) processing is necessary for reasons of substantial public interest, on the basis of Union law, or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests; or
(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or	(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or	(h) processing ~~of data concerning health~~ is necessary for ~~health purposes~~ ***the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law or pursuant to contract with a***	*Presidency suggestion:* (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law or pursuant to contract

		health professional and subject to the conditions and safeguards referred to in ~~Article 81~~***paragraph 4***; or	with a health professional and subject to the conditions and safeguards referred to in paragraph 4; or
		(hb) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject; or	*Presidency suggestion:* (hb) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject; or
(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or	(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or	(i) processing is necessary for ***archiving purposes in the public interest or*** historical, statistical or scientific ~~research~~ purposes ***and*** subject to the conditions and safeguards ***laid down in Union or Member State law, including those*** referred to in Article 83***.***	*Presidency suggestion:* [(i) processing is necessary for archiving purposes in the public interest or historical, statistical or scientific purposes and subject to the conditions and safeguards laid down in Union or Member State law, including those referred to in Article 83.]

	(ia) processing is necessary for archive services subject to the conditions and safeguards referred to in Article 83a; or		
(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.	(j) processing of data relating to ***administrative sanctions, judgments,*** criminal ***offences,*** convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards~~. A complete~~ ***for the fundamental rights and the interests of the data subject***. ***Any*** register of criminal convictions shall be kept only under the control of official authority.	***deleted***	

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.	3. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~***entrusted with the task*** of ~~further specifying the criteria, conditions and appropriate safeguards~~ ***issuing guidelines, recommendations and best practices*** for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2***, in accordance with Article 66***.	***deleted***	
		4. Personal data referred to in paragraph 1 may on the basis of Union or Member State law be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.	*Presidency suggestion:* 4. Personal data referred to in paragraph 1 may on the basis of Union or Member State law be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

		5. Member States may maintain or introduce more specific provisions with regard to genetic data or health data. This includes the possibility for Member States to introduce further conditions for the processing of these data.	*Presidency suggestion:* *delete*
		Article 9a	***Article 9a***
		Processing of data relating to criminal convitions and offences	***Processing of data relating to criminal convitions and offences***
		Processing of data relating to criminal convictions and offences or related security measures based on Article 6(1) may only be carried out either under the control of official authority or when the processing is authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority.	*Tentative agreement in trilogue:* Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) may only be carried out either under the control of official authority or when the processing is authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions may be kept only under the control of official authority.

Article 10	***Article 10***	***Article 10***	***Article 10***
Processing not allowing identification	***Processing not ~~allowing~~ identification***	***Processing not ~~allowing~~ requiring identification***	***Processing not requiring identification***
	Amendment 104		
If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	***1.*** If the data processed by a controller do not permit the controller ***or processor*** to ***directly or indirectly*** identify a natural person, ***or consist only of pseudonymous data,*** the controller shall not ~~be obliged to~~ ***process or*** acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	If the ~~data processed by~~ ***purposes for which a*** controller ***processes personal data*** do not ~~permit~~***or do no longer require the identification of a data subject by*** the controller ~~to identify a natural person~~, the controller shall not be obliged to ***maintain or*** acquire additional information ***nor to engage in additional processing*** in order to identify the data subject for the sole purpose of complying with ~~any provision of~~ this Regulation.	*Tentative agreement in trilogue*: 1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
	2. Where the data controller is unable to comply with a provision of this Regulation because of paragraph 1, the controller shall not be obliged to comply with that particular provision of this Regulation. Where as a consequence the data controller is unable to comply with a request of the data subject, it shall inform the data subject accordingly.	***2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification.***	*Tentative agreement in trilogue:* 2. Where, in such cases the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, articles 15 to 18 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification.

CHAPTER III RIGHTS OF THE DATA SUBJECT	CHAPTER III RIGHTS OF THE DATA SUBJECT	CHAPTER III RIGHTS OF THE DATA SUBJECT	CHAPTER III RIGHTS OF THE DATA SUBJECT
SECTION 1 TRANSPARENCY AND MODALITIES	**SECTION 1 TRANSPARENCY AND MODALITIES**	**SECTION 1 TRANSPARENCY AND MODALITIES**	**SECTION 1 TRANSPARENCY AND MODALITIES**
	Article 10 a (new)		
	Amendment 105		
	General principles for the rights of the data subject ~~rights~~		
	1. The basis of data protection is clear and unambiguous rights for the data subject which shall be respected by the data controller. The provisions of this Regulation aim to strengthen, clarify, guarantee and where appropriate, codify these rights.		

	2. Such rights include, inter alia, the provision of clear and easily understandable information regarding the processing of the data subject's ~~his or her~~ personal data, the right of access, rectification and erasure of ~~their~~ his or her data, the right to obtain data, the right to object to profiling, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.		

Article 11	***Article 11***	***Article 11***	
Transparent information and communication	***Transparent information and communication***	***Transparent information and communication***	
	Amendment 106		
1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.	1. The controller shall have ***concise,*** transparent***, clear*** and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights	***deleted***	
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.	2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, ~~adapted to the data subject,~~ in particular for any information addressed specifically to a child.	***deleted***	

Article 12	*Article 12*	*Article 12*	*Article 12*
Procedures and mechanisms for exercising the rights of the data subject	***Procedures and mechanisms for exercising the rights of the data subject***	**~~Procedures and mechanisms~~ Transparent information, communication and modalities for exercising the rights of the data subject**	***Transparent information, communication and modalities for exercising the rights of the data subject***
	Amendment 107		
1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.	1. ~~The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19.~~ Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically ***where possible***.	1. The controller shall ~~establish procedures for providing the~~ ***take appropriate measured to provide any*** information referred to in Article 14 and ***14a*** ~~for the exercise of the rights of data subjects referred to in Article 13~~ and ***any communication under*** Articles 15 to 19 ***and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, where appropriately in electronic form. Where the data subject makes the request in electronic form, the information may as a rule be provided in electronic form, unless otherwise requested by the data subject. When requested by***	*Tentative agreement in trilogue:*1. The controller shall take appropriate measures to provide any information referred to in Article 14 and 14a and any communication under Articles 15 to 19, and 32 relating to the processing of personal data to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, where appropriately in electronic form. When requested by the data subject, the information may be given orally provided that the identity of the data subject is proven other means.

		the data subject, the information may be given orally provided that the identity of the data subject is proven other means. ~~The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.~~	
		1a. The controller shall facilitate the exercise of data subject rights under Articles 15 to 19. In cases referred to in Article 10 (2) the controller shall not refuse to act on the request of the data subject for exercising his/her rights under Articles 15 to 19, unless the controller demonstrates that he/she is not in a position to identify the data subject.	*Tentative agreement in trilogue:* 1a. The controller shall facilitate the exercise of data subject rights under Articles 15 to 20.

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.	2. The controller shall inform the data subject without ***undue*** delay and, at the latest within ~~one month~~ ***40 calendar days*** of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing ***and, where possible, the controller may provide remote access to a secure system which would provide the data subject with direct access to ~~their~~ his or her personal data***. Where the data subject makes the request in electronic form, the information shall be provided in electronic form ***where possible***, unless otherwise requested by the data subject.	2. The controller shall ***provide*** inform***ation on action taken on a request under Articles 15 and 16 to 19 to*** the data subject without ***undue*** delay and, at the latest within one month of receipt of the request~~, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information~~. This period may be ~~prolonged~~ ***extended*** for a further ***two*** month***s when necessary, taking into account the complexity of the request and the number of the requests.***~~, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing.~~ Where ***the extended period applies,*** the data subject ~~makes the request in electronic form, the information~~ shall be ~~provided in electronic form, unless otherwise requested by the data subject~~***informed within one month of receipt of the request of the reasons for the delay***.	*Tentative agreement in trilogue:* 2. The controller shall provide information on action taken on a request under Articles 15 to 20 to the data subject without undue delay and, at the latest within one month of receipt of the request. This period may be extended for a maximum of two further months when necessary, taking into account the complexity of the request and the number of the requests. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay. Where the data subject makes the request in electronic form, the information shall be provided in electronic form where possible, unless otherwise requested by the data subject.

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	3. If the controller ~~refuses to~~ ***does not*** take action at the request of the data subject, the controller shall inform the data subject of the reasons for the ~~refusal~~***inaction*** and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.	3. If the controller ~~refuses to~~***does not*** take action on the request of the data subject, the controller shall inform the data subject ***without delay and at the latest within one month of receipt of the request*** of the reasons for ~~the refusal~~***not taking action*** and on the ~~possibilities~~ ***possibility*** of lodging a complaint to ~~the~~ ***a*** supervisory authority ~~and seeking a judicial remedy~~.	*Tentative agreement in trilogue:* 3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint to a supervisory authority and seeking a judicial remedy.
4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.	4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a ***reasonable*** fee ***taking into account the administrative costs*** for providing the information or taking the action requested~~, or the controller may not take the action requested~~. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.	4. ~~The i~~***I***nformation ~~and the actions taken on requests referred to in paragraph 1~~***provided under Articles 14 and 14a and any communication under Articles 16 to 19 and 32*** shall be ***provided*** free of charge. Where requests ***from a data subject*** are manifestly ***unfounded or*** excessive, in particular because of their repetitive character, the controller may ~~charge a fee for providing the information or taking the action requested, or the controller may not take the action requested~~ ***refuse to act on***	*Tentative agreement in trilogue:* 4. Information provided under Articles 14 and 14a and any communication and any actions taken under Articles 15 to [19/20] and 32 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee taking into account the

		the request. In that case, the controller shall bear the burden of ~~proving~~ ***demonstrating*** the manifestly ***unfounded or*** excessive character of the request.	administrative costs for providing the information or the communication or taking the action requested, or the controller may refuse to act on the request. In these cases, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
		4a. Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	*Tentative agreement in trilogue:* 4a. Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.	***deleted***	***deleted***	

			Presidency suggestion: 4b. The information to be provided to data subjects pursuant to Article 14 and 14a may be provided by, amongst others or in combination with, standardised icons in order to give in an easily visible, intelligible and clearly legible way a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.
			Presidency suggestion: 4c. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Article 13	*Article 13*	*Article 13*	
	Amendment 108		
Rights in relation to recipients	***~~Rights in relation to recipients~~ Notification requirement in the event of rectification and erasure***	***Rights in relation to recipients***	
The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.	The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been ~~disclosed~~ ***transferred***, unless this proves impossible or involves a disproportionate effort. ***The controller shall inform the data subject about those recipients if the data subject requests this.***	***deleted***	

SECTION 2	SECTION 2	SECTION 2	SECTION 2
INFORMATION AND ACCESS TO DATA	**INFORMATION AND ACCESS TO DATA**	**INFORMATION AND ACCESS TO DATA**	**INFORMATION AND ACCESS TO DATA**
	Article 13 a (new)		
	Amendment 109		
	Standardised information policies		
	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following particulars before providing information pursuant to Article 14:		
	(a) whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;		
	(b) whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;		
	(c) whether personal data are processed for purposes other than the purposes for which they were collected;		
	(d) whether personal data are disseminated to commercial third parties;		

	(e) whether personal data are sold or rented out;		
	(f) whether personal data are retained in encrypted form.		
	2. The particulars referred to in paragraph 1 shall be presented pursuant to Annex to this Regulation in an aligned tabular format, using text and symbols, in the following three columns:		
	(a) the first column depicts graphical forms symbolising those particulars;		
	(b) the second column contains essential information describing those particulars;		
	(c) the third column depicts graphical forms indicating whether a specific particular is met.		
	3. The information referred to in paragraphs 1 and 2 shall be presented in an easily visible and clearly legible way and shall appear in a language easily understood by the consumers of the Member States to whom the information is provided. Where the particulars are presented electronically, they shall be machine readable.		

	4. Additional particulars shall not be provided. Detailed explanations or further remarks regarding the particulars referred to in paragraph 1 may be provided together with the other information requirements pursuant to Article 14.		
	5. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying the particulars referred to in paragraph 1 and their presentation as referred to in paragraph 2 and in the Annex to this Regulation.		

~~*Article 14*~~	*Article 14*	*Article 14*	*Article 14*
Information to the data subject	***Information to the data subject***	***Information to be provided where the data are collected from the data subject***	***Information to be provided where the data are collected from the data subject***
	Amendment 110		
1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information, ***after the particulars pursuant to Article 13a have been provided***:	1. Where personal data relating to a data subject are collected ***from the data subject***, the controller shall***, at the time when personal data are obtained,*** provide the data subject with ~~at least~~ the following information:	*Tentative agreement in trilogue:* 1. Where personal data relating to a data subject are collected from the data subject, the controller shall***,*** at the time when personal data are obtained, provide the data subject with the following information:
(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;	(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer**;**	(a) the identity and the contact details of the controller and, if any, of the controller's representative***; the controller shall also include the contact details*** ~~and~~ of the data protection officer***, if any***;	*Tentative agreement in trilogue:*(a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller shall also include the contact details of the data protection officer, if any;

(b) the purposes of the processing for which the personal data are intended, ***including the contract terms and general conditions where the processing is based on point (b) of Article 6(1)*** and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	(b) the purposes of the processing for which the personal data are intended, ***as well as information regarding the security of the processing of personal data,*** including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and ~~the legitimate interests pursued by the controller where the processing is based on~~ ***, where applicable, information on how they implement and meet the requirements of*** point (f) of Article 6(1);	(b) the purposes of the processing for which the personal data are intended~~, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);~~ ***as well as the legal basis of the processing.***	*Tentative agreement in trilogue:*(b) the purposes of the processing for which the personal data are intended as well as the legal basis of the processing.
		1a. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with such further information that is necessary to ensure fair and transparent processing, having regard to the specific circumstances and context in which the personal data are processed:	*Presidency suggestion:* 1a. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(c) the period for which the personal data will be stored;	(c) the period for which the personal data will be stored***, or if this is not possible, the criteria used to determine this period***;	***deleted***	*Tentative agreement in trilogue:*(a) the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
		(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;	*Presidency suggestion:* (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
		(~~f~~c) the recipients or categories of recipients of the personal data;	*Tentative agreement in trilogue:* (c) the recipients or categories of recipients of the personal data;

		(gd) where applicable, that the controller intends to transfer ***personal data*** to a ***recipient in a*** third country or international organisation ~~and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission~~;	*Tentative agreement in trilogue:* (d) where applicable, that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in case of transfers referred to in Article 42 or 43, or point (h) of Article 44(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;	(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject***,*** ~~or~~ to object to the processing of such personal data***, or to obtain data***;	(~~d~~***e***) the existence of the right to request from the controller access to and rectification or erasure of the personal data ***or restriction of processing of personal data*** concerning the data subject ~~or~~ ***and*** to object to the processing of such personal data ***as well as the right to data portability***;	*Tentative agreement in trilogue:* (e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject or to object to the processing of such personal data as well as the right to data portability;

		(ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	*Tentative agreement in trilogue:* (ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	(e) the right to lodge a complaint ~~to~~***with*** the supervisory authority and the contact details of the supervisory authority;	(~~e~~***f***) the right to lodge a complaint to ~~the~~ ***a*** supervisory authority~~ and the contact details of the supervisory authority~~;	*Tentative agreement in trilogue:*(f) the right to lodge a complaint to a supervisory authority;
(f) the recipients or categories of recipients of the personal data;	(f) the recipients or categories of recipients of the personal data;	*moved under (c)*	*moved under (c)*

(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;	(g) where applicable, that the controller's intends to transfer ***the data*** to a third country or international organisation and ~~on the level of protection afforded by that third country or international organisation by reference to~~ ***the existence or absence of*** an adequacy decision by the Commission***, or in case of transfers referred to in Article 42~~, Article~~or 43~~, or point (h) of Article 44(1)~~, reference to the appropriate safeguards and the means to obtain a copy of them***;	*moved under (d) modified*	*moved under (d) modified*
		(g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the data and of the possible consequences of failure to provide such data;	*Tentative agreement in trilogue:*(g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the data and of the possible consequences of failure to provide such data;

	(ga) where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;		
	(gb) meaningful information about the logic involved in any automated processing;		
		(h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) and information concerning the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	*Presidency suggestion:* (h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	(h) any further information ***which is*** necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected ***or processed, in particular the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk;***	***deleted***	
	(ha) where applicable, information whether personal data ~~was~~ were provided to public authorities during the last consecutive 12-month period.		

		1b. Where the controller intends to further process the data for a purpose other than the one for which the data were collected the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 1a.	*Presidency suggestion:*1b. Where the controller intends to process the data for another purpose than the one for which the data were collected the controller shall provide the data subject prior to that processing with information on that other purpose and with any relevant further information as referred to in paragraph 1a**.**
2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.	2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is ~~obligatory~~ ***mandatory*** or ~~voluntary~~***optional***, as well as the possible consequences of failure to provide such data.	***deleted***	

	2a. In deciding on further information which is necessary to make the processing fair under point (h) of paragraph 1, controllers shall have regard to any relevant guidance under Article ~~38~~34.		
3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.	3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the ***specific*** personal data originate. ***If personal data originate from publicly available sources, a general indication may be given.***	***deleted***	
4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:	4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:	***deleted***	
(a) at the time when the personal data are obtained from the data subject; or	(a) at the time when the personal data are obtained from the data subject ***or without undue delay where the above is not feasible***; or	***deleted***	

	(aa) ~~on~~ at the request ~~by~~ of a body, organization or association referred to in Article 73;		
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.	(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a ~~disclosure~~ ***transfer*** to another recipient is envisaged, and at the latest ~~when the data are first disclosed.~~***at the time of the first transfer, or, if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject; or***	***deleted***	
	(ba) only on request where the data are processed by a small or micro enterprise which processes personal data only as an ancillary activity.		

5. Paragraphs 1 to 4 shall not apply, where:	5. Paragraphs 1 to 4 shall not apply, where:	5. Paragraphs 1***, ~~to 4~~1a and 1b*** shall not apply~~,~~ where ***and insofar as the data subject already has the information.***	*Tentative agreement in trilogue:* 5. Paragraphs 1, 1a and 1b shall not apply where and insofar as the data subject already has the information.
(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or	(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or	*merged with above 5.*	*merged with above 5.*
(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or	(b) the data ***are processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83,*** are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort ***and the controller has published the information for anyone to retrieve***; or	***deleted***	

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or	(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law ***to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests, considering the risks represented by the processing and the nature of the personal data***; or	***deleted***	
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of ~~others~~ ***other natural persons***, as defined in Union law or Member State law in accordance with Article 21***;***	***deleted***	
	(da) the data are processed in the exercise of his profession by, or are entrusted or become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation of secrecy, unless the data is collected directly from the data subject.		

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.	6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's ***rights or*** legitimate interests.	***deleted***	
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.	***deleted***	***deleted***	

8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

		Article 14a	***Article 14a***
		Information to be provided where the data have not been obtained from the data subject	***Information to be provided where the data have not been obtained from the data subject***
		1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:	*Tentative agreement in trilogue:* 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
		(a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller shall also include the contact details of the data protection officer, if any;	*Tentative agreement in trilogue:* (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller shall also include the contact details of the data protection officer, if any;
		(b) the purposes of the processing for which the personal data are intended as well as the legal basis of the processing.	*Tentative agreement in trilogue:* (b) the purposes of the processing for which the personal data are intended as well as the legal basis of the processing.

		2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information that is necessary 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 :	*Presidency suggestion:* 2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:
		(a) the categories of personal data concerned;	*Tentative agreement in trilogue:* (a) the categories of personal data concerned;
			Tentative agreement in trilogue: (b) the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
		(c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;	*Presidency suggestion:* (c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

		(d) the recipients or categories of recipients of the personal data;	*Tentative agreement in trilogue:* (d) the recipients or categories of recipients of the personal data;
		(da) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisatio;	*Tentative agreement in trilogue:* (da) where applicable, that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in case of transfers referred to in Article 42 or 43, or point (h) of Article 44(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;
		(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject and to object to the processing of such personal data as well as the right to data portability;	*Tentative agreement in trilogue:* (e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject and to object to the processing of such personal data as well as the right to data portability;

		(ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	*Tentative agreement in trilogue:* (ea) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
		(f) the right to lodge a complaint to a supervisory authority;	*Tentative agreement in trilogue:* (f) the right to lodge a complaint to a supervisory authority;
		(g) from which source the personal data originate, unless the data originate from publicly accessible sources;	*Presidency suggestion:* (g) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

		(h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) and information concerning the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	*Tentative agreement in trilogue:* (h) the existence of automated decision making including profiling referred to in Article 20[(1) and (3)] and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
		3. The controller shall provide the information referred to in paragraphs 1 and 2:	*Tentative agreement in trilogue:* 3. The controller shall provide the information referred to in paragraphs 1 and 2:
		(a) within a reasonable period after obtaining the data, but at the latest within one month, having regard to the specific circumstances in which the data are processed, or	*Tentative agreement in trilogue:* (a) within a reasonable period after obtaining the data, but at the latest within one month, having regard to the specific circumstances in which the data are processed, or

			Tentative agreement in trilogue: (b) if the data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
		(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.	*Tentative agreement in trilogue:* (c) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.
		3a. Where the controller intends to further process the data for a purpose other than the one for which the data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2	*Tentative agreement in trilogue:* 3a. Where the controller intends to process the data for another purpose other than the one for which the data were obtained, the controller shall provide the data subject prior to that processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

		4. Paragraphs 1 to 3a shall not apply where and insofar as:	*Tentative agreement in trilogue:* 4. Paragraphs 1 to 3a shall not apply where and insofar as:
		(a) the data subject already has the information; or	*Tentative agreement in trilogue:* (a) the data subject already has the information; or
		(b) the provision of such information proves impossible or would involve a disproportionate effort; in such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests; or	*Tentative agreement in trilogue:* (b) the provision of such information proves impossible or would involve a disproportionate effort; in particular for processing [for archiving purposes or for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81, 83, and 83a]; in such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; or

		(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests; or	*Tentative agreement in trilogue:* (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests; or
		(e) where the data must remain confidential in accordance with Union or Member State law .	*Presidency suggestion:* (d) where the data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15	***Article 15***	***Article 15***	***Article 15***
	Amendment 111		
Right of access for the data subject	Right ~~of~~ ***to*** access ***and to obtain data*** for the data subject	***Right of access for the data subject***	***Right of access for the data subject***
1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:	1. ~~The~~***Subject to Article 12(4), the*** data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed~~. Where such personal data are being processed,~~ ***and, in clear and plain language,*** ~~the controller shall provide~~ the following information:	1. The data subject shall have the right to obtain from the controller at ***reasonable intervals and free of charge*** ~~any time, on request,~~ confirmation as to whether or not personal data ~~relating to the data subject~~ ***concerning him or her*** are being processed ***and*** ~~. W~~***w***here such personal data are being processed~~, the controller shall provide~~***access to the data and*** the following information:	*Tentative agreement in trilogue:*1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where such personal data are being processed, access to the data and the following information:
(a) the purposes of the processing;	(a) the purposes of the processing ***for each category of personal data;***	(a) the purposes of the processing;	*Tentative agreement in trilogue:* (a) the purposes of the processing;
(b) the categories of personal data concerned;	(b) the categories of personal data concerned;	***deleted***	*Tentative agreement in trilogue:* (b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;	(c) the recipients ~~or categories of recipients~~ to whom the personal data are to be or have been disclosed, ~~in particular~~ ***including*** to recipients in third countries;	(c) the recipients or categories of recipients to whom the personal data ~~are to be or~~ have been ***or will be*** disclosed, in particular to recipients in third countries ***or international organisations***;	*Tentative agreement in trilogue:* (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries or international organisations;
(d) the period for which the personal data will be stored;	(d) the period for which the personal data will be stored***, or if this is not possible, the criteria used to determine this period***;	(d) ***where possible,*** the ***envisaged*** period for which the personal data will be stored;	*Tentative agreement in trilogue:* (d) the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;	(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;	(e) the existence of the right to request from the controller rectification or erasure of personal data ***or restriction of the processing of personal data*** concerning the data subject or to object to the processing of such personal data;	*Tentative agreement in trilogue:* (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of the processing of personal data concerning the data subject or to object to the processing of such personal data;

(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	(f) the right to lodge a complaint ~~to~~ ***with*** the supervisory authority and the contact details of the supervisory authority;	*(*f) the right to lodge a complaint to ***a*** supervisory authority***;***	*Tentative agreement in trilogue:* (f) the right to lodge a complaint to a supervisory authority;
(g) communication of the personal data undergoing processing and of any available information as to their source;	***deleted***	***(g) where*** ~~communication of~~ the personal data ~~undergoing processing and of~~ ***are not collected from the data subject,*** any available information as to their source***;***	*Tentative agreement in trilogue:* (g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.	(h) the significance and envisaged consequences of such processing~~, at least in the case of measures referred to in Article 20.~~***;***	(h) ***in the case of decisions based on automated processing including profiling referred to in Article 20(1) and (3), information concerning the logic involved as well as*** the significance and envisaged consequences of such processing~~, at least in the case of measures referred to in Article 20~~.	*Tentative agreement in trilogue:* (h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
	(ha) meaningful information about the logic involved in any automated processing;		*Covered by (h)*

	(hb) without prejudice to Article 21, in the event of disclosure of personal data to a public authority as a result of a public authority request, confirmation of the fact that such a request has been made.		
		1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer.	*Tentative agreement in trilogue:* 1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer.
		1b. On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject.	*Tentative agreement in trilogue:* 1b. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request in electronic form, and unless otherwise requested by the data subject, the information shall be provided in an electronic form, which is commonly used.

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.	2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in ***an*** electronic ~~form~~ ***and structured format***, unless otherwise requested by the data subject. ***Without prejudice to Article 10, the controller shall take all reasonable steps to verify that the person requesting access to the data is the data subject.***	***deleted*** → *see Article 18 Council text*	

	2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.		
	2b. This Article shall be without prejudice to the obligation to delete data when no longer necessary under point (e) of Article 5(1).		

	2c. There shall be no right of access in accordance with paragraphs 1 and 2 when data within the meaning of point (da) of Article 14(5) are concerned, except if the data subject is empowered to lift the secrecy in question and acts accordingly.		
		2a. The right to obtain a copy referred to in paragraph 1b shall not apply where such copy cannot be provided without disclosing personal data of other data subjects or confidential data of the controller. Furthermore, this right shall not apply if disclosing personal data would infringe intellectual property rights in relation to processing of those personal data.	*Tentative agreement in trilogue:* 2a. The right to obtain a copy referred to in paragraph 1b shall not adversely affect the rights and freedoms of others.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.	***deleted***	***deleted***	

4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

SECTION 3 RECTIFICATION AND ERASURE	SECTION 3 RECTIFICATION AND ERASURE	SECTION 3 RECTIFICATION AND ERASURE	SECTION 3 RECTIFICATION AND ERASURE
Article 16	***Article 16***	***Article 16***	***Article 16***
Right to rectification	***Right to rectification***	***Right to rectification***	***Right to rectification***
The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.	The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.	The data subject shall have the right to obtain from the controller ***without undue delay*** the rectification of personal data ~~relating to them~~ ***concerning him or her*** which are inaccurate. ***Having regard to the purposes for which data were processed,*** ~~The~~ ***the*** data subject shall have the right to obtain completion of incomplete personal data, including by ~~way~~ ***means*** of ~~supplementing~~ ***providing*** a ~~corrective~~ ***supplementary*** statement.	*Tentative agreement in trilogue:* The data subject shall have the right to obtain from the controller without undue delay the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

Article 17	*Article 17*	*Article 17*	*Article 17*
	Amendment 112		
Right to be forgotten and to erasure	***Right to ~~be forgotten and to~~ erasure***	***Right to* erasure and *to be forgotten ~~and to erasure~~***	*Tentative agreement in trilogue:* ***Right to erasure ("right to be forgotten")***
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:	1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her and the abstention from further dissemination of such data, ~~especially in relation to personal data which are made available by the data subject while he or she was a child,~~ ***and to obtain from third parties the erasure of any links to, or copy or replication of, those data*** where one of the following grounds applies:	1. The ~~data subject shall have the right to obtain from the~~ controller ***shall have the obligation to erase*** ~~the erasure of~~ personal data ~~relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by~~ ***without undue delay, especially in relation to personal which are collected when*** the data subject ~~while he or she~~ was a child, ***and the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay*** where one of the following grounds applies:	*Tentative agreement in trilogue:* 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	*Tentative agreement in trilogue:* (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;	(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;	(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or ***point (a) of Article 9(2) and*** ~~when the storage period consented to has expired, and where~~ there is no other legal ground for the processing of the data;	*Tentative agreement in trilogue:* (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing of the data;
(c) the data subject objects to the processing of personal data pursuant to Article 19;	(c) the data subject objects to the processing of personal data pursuant to Article 19;	(c) the data subject objects to the processing of personal data pursuant to Article 19***(1) and there are no overriding legitimate grounds for the processing or the data subject objects to the processing of personal data pursuant to Article 19(2)*** ;	*Tentative agreement in trilogue:* (c) the data subject objects to the processing of personal data pursuant to Article 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data pursuant to Article 19(2);

	(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;		
(d) the processing of the data does not comply with this Regulation for other reasons.	(d) the ~~processing of the~~ data ~~does not comply with this Regulation for other reasons~~ ***~~has~~*** **have** ***been unlawfully processed***.	***(d) the*** ~~processing of the~~ data ~~does not comply with this Regulation for other reasons~~ ***have been unlawfully processed;***	*Tentative agreement in trilogue:*(d) they have been unlawfully processed;
		(e) the data have to be erased for compliance with a legal obligation to which the controller is subject.	*Tentative agreement in trilogue:* (e) the data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
	1a. The application of paragraph 1 shall be dependent upon the ability of the controller to verify that the person requesting the erasure is the data subject.		*Tentative agreement in trilogue:* (f) the data have been collected in relation to the offering of information society services referred to in Article 8(1).

		1a. The data subject shall have also the right to obtain from the controller the erasure of personal data concerning him or her, without undue delay, if the data have been collected in relation to the offering of information society services referred to in Article 8(1).	*moved to new 17(1) (f)*
2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.	2. Where the controller referred to in paragraph 1 has made the personal data public ***without a justification based on Article 6(1)***, it shall take all reasonable steps~~, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication~~ ***to have the data erased, including by third parties, without prejudice to Article 77. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.***	***deleted***	

		2a. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copy or replication of that personal data.	*Tentative agreement in trilogue:* 2a. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copy or replication of that personal data.
3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:	3. The controller ***and, where applicable, the third party*** shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:	3. ~~The controller shall carry out the erasure without delay, except~~ ***Paragraphs 1 and 2a shall not apply*** to the extent that ~~the retention~~ ***processing*** of the personal data is necessary:	*Tentative agreement in trilogue:* 3. Paragraphs 1 and 2 shall not apply to the extent that processing of the personal data is necessary:
(a) for exercising the right of freedom of expression in accordance with Article 80;	(a) for exercising the right of freedom of expression in accordance with Article 80;	(a) for exercising the right of freedom of expression ~~in accordance with Article 80~~ ***and information***;	*Presidency suggestion:* [(a) for exercising the right of freedom of expression and information;]

		(b) ***for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;***	*Tentative agreement in trilogue:* (b) for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(b) for reasons of public interest in the area of public health in accordance with Article 81;	(b) for reasons of public interest in the area of public health in accordance with Article 81;	(~~b~~***c***) for reasons of public interest in the area of public health in accordance with Article ~~81~~***9(2)(h) and (hb) as well as Article 9(4)***;	*Presidency suggestion:* (c) for reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (hb) as well as Article 9(4);
(c) for historical, statistical and scientific research purposes in accordance with Article 83;	(c) for historical, statistical and scientific research purposes in accordance with Article 83;	(~~c~~***d***) for ***archiving purposes in the public interest or for*** **scientific,** historical, statistical and **historical**~~scientific research~~ purposes in accordance with Article 83;	*Presidency suggestion:* [(d) for archiving purposes in the public interest or for scientific, historical, statistical and historical purposes in accordance with Article 83;]

(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;	(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the right to the protection of personal data and be proportionate to the legitimate aim pursued;	***deleted***	
(e) in the cases referred to in paragraph 4.	(e) in the cases referred to in paragraph 4.	***deleted***	
		(g) for the establishment, exercise or defence of legal claims.	*Tentative agreement in trilogue:* (e) for the establishment, exercise or defence of legal claims.
4. Instead of erasure, the controller shall restrict processing of personal data where:	4. Instead of erasure, the controller shall restrict processing of personal data ***in such a way that it is not subject to the normal data access and processing operations and cannot be changed anymore,*** where:	***deleted***	
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;	(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;	***deleted***	

(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;	(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;	***deleted***	
(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;	(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;	***deleted***	
	(ca) a court or regulatory authority based in the Union has ruled as final and absolute **than the processing** ~~***that the data***~~ ***concerned must be restricted;***		
(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).	(d) the data subject requests to transmit the personal data into another automated processing system in accordance with ***paragraphs 2a of*** Article ~~18(2).~~***15;***	***deleted***	
	(da) the particular type of storage technology does not allow for erasure and has been installed before the entry into force of this Regulation.		

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.	5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.	***deleted***	
6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.	6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.	***deleted***	
7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.	***deleted***	***deleted***	
8. Where the erasure is carried out, the controller shall not otherwise process such personal data.	8. Where the erasure is carried out, the controller shall not otherwise process such personal data.	***deleted***	

	8a. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.		
9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:	9. The Commission shall be empowered to adopt***, after requesting an opinion of the European Data Protection Board,*** delegated acts in accordance with Article 86 for the purpose of further specifying:	***deleted***	*Presidency suggestion:* 9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:
(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;	(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;	***deleted***	
(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;	(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;	***deleted***	*Presidency suggestion:* (b) the procedures for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2.

(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	***deleted***	

		Article 17a	***Article 17a***
		Right to restriction of processing	***Right to restriction of processing***
		1. The data subject shall have the right to obtain from the controller the restriction of the processing of personal data where:	*Tentative agreement in trilogue:* 1. The data subject shall have the right to obtain from the controller the restriction of the processing of personal data where:
		(a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;	*Tentative agreement in trilogue:*(a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
			Tentative agreement in trilogue: (ab) the processing is unlawful and the data subject opposes the erasure of the data and requests the restriction of their use instead;

		(b) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or	*Tentative agreement in trilogue:* (b) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
		(c) he or she has objected to processing pursuant to Article 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	*Presidency suggestion:* (c) he or she has objected to processing pursuant to Article 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
		2. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.	*Tentative agreement in trilogue:* 2. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

		3. A data subject who obtained the restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.	*Tentative agreement in trilogue:* 3. A data subject who obtained the restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

		Article 17b	***Article 17b***
		Notification obligation regarding rectification, erasure or restriction	***Notification obligation regarding rectification, erasure or restriction***
		The controller shall communicate any rectification, erasure or restriction of processing carried out in accordance with Articles 16, 17(1) and 17a to each recipient to whom the data have been disclosed, unless this proves impossible or involves disproportionate effort.	*Tentative agreement in trilogue:* The controller shall communicate any rectification, erasure or restriction of processing carried out in accordance with Articles 16, 17(1) and 17a to each recipient to whom the data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests this.

Article 18	*Article 18*	*Article 18*	*Article 18*
	Amendment 113		
Right to data portability	***Right to data portability***	***Right to data portability***	***Right to data portability***
1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.	***deleted***	***deleted***	
2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	***deleted***	2. ~~Where t~~***T***he data subject ~~has provided~~ ***shall have the right to receive*** the personal data ***concerning him or her, which he or she has provided*** ~~and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, in~~to ~~another one, in an electronic format which is~~ ***to a ontroller, in a***	*Tentative agreement in trilogue:*2. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided, where:

		structured and commonly used ***and machine-readable format and have the right to transmit those data to another controller*** without hindrance from the controller ~~from whom the personal data are withdrawn~~ ***to which the data have been provided, where***:	
		(a) the processing is based on consent pursuant to point (a) of Article 6(1)or point (a) of Article 9 (2) or on a contract pursuant to point (b) of Article 6 (1); and	*Tentative agreement in trilogue:* (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9 (2) or on a contract pursuant to point (b) of Article 6 (1); and
		(b) the processing is carried out by automated means.	*Tentative agreement in trilogue:* (b) the processing is carried out by automated means
			Presidency suggestion: 2a (new). Where technically feasible and available, the data may be transferred directly from controller to controller at the request of the data subject.

		2a. The exercise of this right shall be without prejudice to Article 17. The right referred to in paragraph 2 shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	*Tentative agreement in trilogue:* 3. The exercise of this right shall be without prejudice to Article 17. The right referred to in paragraph 2 shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
		2aa. The right referred to in paragraph 2 shall not apply if disclosing personal data would infringe intellectual property rights in relation to the processing of those personal data.	*Tentative agreement in trilogue:* 2aa. The right referred to in paragraph 2 shall not adversely affect the rights and freedoms of others.
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

SECTION 4 RIGHT TO OBJECT AND PROFILING	SECTION 4 RIGHT TO OBJECT AND PROFILING	SECTION 4 RIGHT TO OBJECT AND ~~PROFILING~~ *AUTOMATED INDIVIDUAL DECISION MAKING*	*SECTION 4* *RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION MAKING*
Article 19	***Article 19***	***Article 19***	***Article 19***
Right to object	***Right to object***	***Right to object***	***Right to object***
	Amendment 114		
1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.	1. The data subject shall have the right to object~~, on grounds relating to their particular situation,~~ at any time to the processing of personal data which is based on points (d)~~,~~ ***and*** (e) ~~and (f)~~ of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject**.**	1. The data subject shall have the right to object, on grounds relating to ~~their~~ ***his or her*** particular situation, at any time to the processing of personal data ***concerning him or her*** which is based on points (e) ~~and~~ ***or*** (f) of Article 6(1)***; the first sentence of Article 6(4) in conjunction with point (e) of Article 6(1) or the second sentence of Article 6(4). The controller shall*** **no longer process** ***the personal data*** unless the controller demonstrates compelling legitimate grounds for the processing which override the	*Presidency suggestion:* 1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on these provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the

		interests**,** ~~or fundamental~~ rights and freedoms of the data subject ***or for*** **the establishment, exercise or defence of legal claims**.	interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.	2. Where ***the processing of*** personal data ~~are processed for direct marketing purposes~~ ***is based on point (f) of Article 6(1)***, the data subject shall have, ***at any time and without any further justification,*** the right to object free of charge ***in general or for any particular purpose*** to the processing of his or her personal data ~~for such marketing~~. ~~This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.~~	2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object ~~free of charge~~ ***at any time*** to the processing of ~~their~~ personal data ***concerning him or her*** for such marketing. ***At the latest at the time of the first communication with the data subject,*** ~~T~~***t***his right shall be explicitly ~~offered to~~ ***brought to the attention of*** the data subject ~~in an intelligible manner~~ and shall be ~~clearly distinguishable~~ ***presented clearly and separately*** from ***any*** other information.	*Presidency suggestion:* 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing. At the latest at the time of the first communication with the data subject, this right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
	2a. The right referred to in paragraph 2 shall be explicitly offered to the data subject in an intelligible manner and form, using clear and plain language, in particular if addressed specifically to a child, and shall be clearly distinguishable from other information.		

		2a. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	*Tentative agreement in trilogue:* 2a. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
	2b. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the right to object may be exercised by automated means using a technical standard which allows the data subject to clearly express his or her wishes.		*Presidency suggestion:* 2b. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
		2aa. Where personal data are processed for historical, statistical or scientific purposes the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.	*Presidency suggestion:* [2aa. Where personal data are processed for historical, statistical or scientific purposes the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.]

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.	3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned ***for the purposes determined in the objection***.	***deleted***	

Article 20	*Article 20*	*Article 20*	*Article 20*
	Amendment 115		
Measures based on profiling	~~***Measures based on profiling***~~***Profiling***	~~***Measures based on profiling***~~**Automated individual decision making**	**Automated individual decision making, including profiling**
1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.	1. ***Without prejudice to the provisions in Article 6,*** ~~Every~~ ***every*** natural person shall have the right ***to object*** ~~not~~ to ~~be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour~~ ***profiling in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.***	1. ~~Every natural person~~ ***The data subject*** shall have the right not to be subject to a ~~measure which produces legal effects concerning this natural person or significantly affects this natural person, and which~~ ***decision*** ~~is~~based solely on automated processing,~~intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour~~***including profiling, which produces legal effects concerning him or her or significantly affects him or her***.	*Presidency suggestion:* 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

		1a. Paragraph 1 shall not apply if the decision:	*Presidency suggestion:* 1a. Paragraph 1 shall not apply if the decision:
		(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ; or	*Presidency suggestion:* (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ; or
		(b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	*Presidency suggestion:* (b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
		(c) is based on the data subject's explicit consent.	*Presidency suggestion:* (c) is based on the data subject's explicit consent.
		1b. In cases referred to in paragraph 1a (a) and (c) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests,	*Presidency suggestion:* 1b. In cases referred to in paragraph 1a (a) and (c) the data controller shall implement suitable measures to safeguard the data

		at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:	2. Subject to the other provisions of this Regulation, a person may be subjected to ~~a measure of the kind referred to in paragraph 1~~ ***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*** only if the processing:	***deleted***	
(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or	(a) is ~~carried out in the course of~~ ***necessary for*** the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied ~~or where~~***, provided that*** suitable measures to safeguard the data subject's legitimate interests have been adduced~~, such as the right to obtain human intervention~~; or	***deleted***	

b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or	(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests;	***deleted***	
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.	(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.	***deleted***	
3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.	***3.*** ~~Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person~~***Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling*** shall not be based solely on the special categories of personal data referred to in Article 9.	~~3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person~~ ***Decisions referred to in paragraph 1a*** shall not be based ~~solely~~ on ~~the~~ special categories of personal data referred to in Article 9***(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.***	*Presidency suggestion:* 3. Decisions referred to in paragraph 1a shall not be based on special categories of personal data referred to in Article 9(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.	***deleted***	***deleted***	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	***5.*** ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for~~ ***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 shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The*** suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 ***shall include the right to obtain human assessment and an explanation of the decision reached after such assessment.***	***deleted***	

	5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for further specifying the criteria and conditions for profiling pursuant to paragraph 2.		*Moved to Article 66*

CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR
SECTION 1 GENERAL OBLIGATIONS	**SECTION 1 GENERAL OBLIGATIONS**	**SECTION 1 GENERAL OBLIGATIONS**	**SECTION 1 GENERAL OBLIGATIONS**
Article 22	***Article 22***	***Article 22***	***Article 22***
	Amendment 117		
Responsibility of the controller	***Responsibility* and accountability *of the controller***	***~~Responsibility~~* Obligations *of the controller***	***Responsibility of the controller***
1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller shall adopt ***appropriate*** policies and implement appropriate ***an demonstrable technical and organisational*** measures to ensure and be able to demonstrate ***in a transparent manner*** that the processing of personal data is performed in compliance with this Regulation, ***having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of processing, the risks for the rights and freedoms of the data subjects and the type of the organisation,***	1. ***Taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals,*** ~~T~~the controller shall ~~adopt policies and~~ implement appropriate measures ~~to ensure~~ and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	*Tentative agreement in trilogue:* 1. Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary.

	both at the time of the determination of the means for processing and at the time of the processing itself.		
	1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary.		
2. The measures provided for in paragraph 1 shall in particular include:	***deleted***	***deleted***	
(a) keeping the documentation pursuant to Article 28;	***deleted***	***deleted***	
(b) implementing the data security requirements laid down in Article 30;	***deleted***	***deleted***	
(c) performing a data protection impact assessment pursuant to Article 33;	***deleted***	***deleted***	
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	***deleted***	***deleted***	

(e) designating a data protection officer pursuant to Article 35(1).	***deleted***	***deleted***	
		2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	*Tentative agreement in trilogue:* 2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
		2b. 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.	*Presidency suggestion:* 2b. 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.
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.	3. The controller shall ~~implement mechanisms to ensure the verification of the~~***be able to demonstrate the adequacy and*** effectiveness of the measures referred to in paragraphs 1 and 2. ~~If proportionate, this verification shall be carried out by independent internal or external auditors~~ ***Any regular general reports of the activities of the controller, such as the obligatory***	***deleted***	

	reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1.		
	3a. The controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct as referred to in Article 38.		

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

Article 23	*Article 23*	*Article 23*	*Article 23*
Data protection by design and by default	***Data protection by design and by default***	***Data protection by design and by default***	***Data protection by design and by default***
	Amendment 118		
1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	1. Having regard to the state of the art ~~and the cost of implementation~~, ***current technical knowledge, international best practices and the risks represented by the data processing,*** the controller ***and the processor, if any,*** shall, both at the time of the determination of the ***purposes and*** means for processing and at the time of the processing itself, implement appropriate ***and proportionate*** technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject***, in particular with regard to the principles laid down in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing***	1. Having regard to ***available technology*** ~~the state of the art~~ and the cost of implementation ***and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing,*** the controller***s*** shall***,*** ~~both at the time of the determination of the means for processing and at the time of the processing itself,~~ implement ~~appropriate~~ technical and organisational measures ***appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation,*** ~~and procedures~~ in such a way that the processing will meet the requirements of this Regulation and ~~ensure~~ ***protect*** ~~the protection of~~ the rights of ~~the~~ data subject***s***.	*Tentative agreement in trilogue:* 1. Having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall***,*** both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

	on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures.		
	1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a prerequisite for public procurement tenders according to Directive 2004/18/EC of the European Parliament and of the Council[1] as well as according to Directive 2004/17/EC of the European Parliament and of the Council[2] (Utilities Directive). ***[1] Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (OJ L 134, 30.4.2004, p. 114).*** ***[2] Directive 2004/17/EC of the***		

	European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sector (OJ L 134, 30.4.2004, p.1)		
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. The controller shall ~~implement mechanisms for ensuring~~ ***ensure*** that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected ~~or~~***,*** retained ***or disseminated*** beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals ***and that data subjects are able to control the distribution of their personal data***.	2. The controller shall implement ~~mechanisms~~ ***appropriate measures*** for ensuring that, by default, only ~~those~~ personal data ~~are processed~~ which are necessary for each specific purpose of the processing ~~and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of~~ ***are processed; this applies to*** the amount of ~~the~~ data ***collected, the extent of their processing,*** ~~and~~ the ~~time~~ ***period*** of their storage ***and their accessibility***. ***Where the purpose of the processing is not intended to provide the public with information*** ~~In particular~~, those mechanisms shall ensure that by default personal data are not made accessible ***without human intervention*** to an indefinite number of individuals.	*Tentative agreement in trilogue:* 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing***,*** the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of individuals.

		2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.	*Presidency suggestion:* 2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.	***deleted***	***deleted***	

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	
Article 24	***Article 24***	***Article 24***	***Article 24***
Joint controllers	***Joint controllers***	***Joint controllers***	***Joint controllers***
	Amendment 119		
Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	Where ~~a controller determines~~ ***several controllers jointly determine*** the purposes~~,~~ ~~conditions~~ and means of the processing of personal data ~~jointly with others~~, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. ***The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the***	***1.*** Where ***two or more*** ~~a~~controller***s jointly*** determine~~s~~ the purposes~~,~~ ~~conditions~~ and means of the processing of personal data ~~jointly with others,~~ the***y are*** joint controllers. ***They*** shall ***in a transparent manner*** determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the ~~procedures and mechanisms for~~ exercising ***of*** the rights of the data subject ***and their respective duties to provide the information referred to in Articles 14 and 14a***, by means of an arrangement between them ***unless, and in so far as, the respective responsibilities of the controllers***	*Tentative agreement in trilogue:* 1. Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union

	arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable.	***are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights***.	or Member State law to which the controllers are subject. The arrangement may designate a point of contact for data subjects.
		2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.	*Tentative agreement in trilogue:* 2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.
		3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. Paragraph 2 does not apply where the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible, unless such arrangement other than one determined by Union or Member State law is unfair with regard to his or her rights.	*Tentative agreement in trilogue:* 3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject.

Article 25	*Article 25*	*Article 25*	*Article 25*
Representatives of controllers not established in the Union	***Representatives of controllers not established in the Union***	***Representatives of controllers not established in the Union***	***Representatives of controllers not established in the Union***
1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.	1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.	1. ~~In the situation referred to in~~ ***Where*** Article 3(2) ***applies***, the controller shall designate ***inwriting*** a representative in the Union.	*Tentative agreement in trilogue:* 1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
2. This obligation shall not apply to:	2. This obligation shall not apply to:	2. This obligation shall not apply to:	*Tentative agreement in trilogue:* 2. This obligation shall not apply to:
(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or	(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or	***deleted***	
(b) an enterprise employing fewer than 250 persons; or	(b) ~~an enterprise employing fewer than 250 persons~~***a controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-month period and not processing 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;*** or	(b) ~~an enterprise employing fewer than 250~~ ***persons processing which is occasional and unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing;*** *or*	*Presidency suggestion:* (b) processing which is occasional, does not include processing of special categories of data as referred to in Article 9(1) or processing of data relating to criminal convictions and offences

			referred to in Article 9a, and is unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing; or
(c) a public authority or body; or	(c) a public authority or body; or	(c) a public authority or body; or	*Tentative agreement in trilogue:* (c) a public authority or body; or
(d) a controller offering only occasionally goods or services to data subjects residing in the Union.	(d) a controller ~~offering~~ only occasionally ***offering*** goods or services to data subjects ~~residing~~ in the Union***, unless the processing of personal data concerns 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***.	***deleted***	
3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.	3. The representative shall be established in one of those Member States where ~~the data subjects whose personal data are processed in relation to~~ the offering of goods or services to ~~them~~***the data subjects***, or ~~whose behaviour is monitored, reside~~ ***the monitoring of them***, ***takes place***.	3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.	*Tentative agreement in trilogue:* 3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.

		3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.	*Tentative agreement in trilogue:* 3a. The representative shall be mandated by the controller or the processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.
4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	*Tentative agreement in trilogue:* 4. The designation of a representative by the controller or the processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 26	***Article 26***	***Article 26***	***Article 26***
Processor	***Processor***	***Processor***	***Processor***
	Amendment 121		
1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. Where ~~a~~ processing ~~operation~~ is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organisational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. ~~Where a processing operation is to be carried out on behalf of a controller, the~~ ***The*** controller shall ~~choose~~ ***use only*** ~~a~~processor***s*** providing sufficient guarantees to implement appropriate technical and organisational measures ~~and procedures~~ in such a way that the processing will meet the requirements of this Regulation~~and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures~~.	*Tentative agreement in trilogue:* 1. Where a processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

		1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.	*Tentative agreement in trilogue:* 1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:	2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller***. The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that*** ~~and stipulating in particular that~~ the processor shall:	2. The carrying out of processing by a processor shall be governed by a contract or ~~other~~ ***a*** legal act ***under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the rights of*** ~~binding the processor to~~ the controller and stipulating in particular that the processor shall:	*Tentative agreement in trilogue:* 2. The carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;	(a) ~~act~~ ***process personal data*** only on instructions from the controller, ~~in particular, where the transfer of the personal data used is prohibited~~***, unless otherwise required by Union law or Member State law***;	(a) ***process the personal data*** ~~act~~ only on instructions from the controller,~~in particular, where the transfer of the personal data used is prohibited~~ ***unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest***;	*Tentative agreement in trilogue:* (a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;
(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	***deleted***	*Tentative agreement in trilogue:* (b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) take all required measures pursuant to Article 30;	(c) take all required measures pursuant to Article 30;	(c) take all ~~required~~ measures **required** pursuant to Article 30;	*Tentative agreement in trilogue:* (c) take all measures required pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;	(d) ~~enlist~~ ***determine the conditions for enlisting*** another processor only with the prior permission of the controller***, unless otherwise determined***;	(d) ***respect the conditions for*** enlist***ing*** another processor ~~only with the prior permission~~ ***such as a requirement of specific prior permission*** of the controller;	*Tentative agreement in trilogue:* (d) respect the conditions referred to in paragraphs 1a and 2a for enlisting another processor;
(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the ~~necessary~~ ***appropriate and relevant*** technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	(e) ~~insofar as this is possible given~~ **taking into account** the nature of the processing, ***assist*** ~~create in agreement with~~ the controller ~~the necessary technical and organisational requirements for the fulfilment of the controller's obligation to~~ ***in*** respond***ing*** to requests for exercising the data subject's rights laid down in Chapter III;	*Tentative agreement in trilogue:* (e) taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34***, taking into account the nature of processing and the information available to the processor***;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	*Tentative agreement in trilogue:* (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34 taking into account the nature of processing and the information available to the processor;

(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;	(g) ~~hand over~~ ***return*** all results to the controller after the end of the processing***,*** ~~and~~ not process the personal data otherwise ***and delete existing copies unless Union or Member State law requires storage of the data;***	(g) ~~hand over all results to~~ ***return or delete, at the choice of*** the controller ~~after the end of the processing and not process~~ the personal data ~~otherwise~~ ***upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject***;	*Tentative agreement in trilogue:* (g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of data processing services, and delete existing copies unless Union or Member State law requires storage of the data;
(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.	(h) make available to the controller ~~and the supervisory authority~~ all information necessary to ~~control~~ ***demonstrate*** compliance with the obligations laid down in this Article ***and allow on-site inspections;***	(h) make available to the controller ~~and the supervisory authority~~ all information necessary to ~~control~~ ***demonstrate*** compliance with the obligations laid down in this Article ***and allow for and contribute to audits conducted by the controller***. ***The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.***	*Tentative agreement in trilogue:* (h) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.

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

		2aa. Adherence of the processor to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate sufficient guarantees referred to in paragraphs 1 and 2a.	*Presidency suggestion:* 2aa. Adherence of the processor to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate sufficient guarantees referred to in paragraphs 1 and 2a.
		2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.	*Presidency suggestion:* 2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a certification granted to the controller or processor pursuant to Articles 39 and 39a.

		2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2).	*Tentative agreement in trilogue:* 2b. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the examination procedure referred to in Article 87(2).
		2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.	*Tentative agreement in trilogue:* 2c. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 2 and 2a and in accordance with the consistency mechanism referred to in Article 57.
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	3. ~~The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2~~ ***The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form***.	*Tentative agreement in trilogue:* 3. The contract or the other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form.

	3a. The sufficient guarantees referred to in paragraph 1 may be demonstrated by adherence to codes of conduct or certification mechanisms pursuant to Articles 38 or 39 of this Regulation.		
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	4. If a processor processes personal data other than as instructed by the controller ***or becomes the determining party in relation to the purposes and means of data processing***, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	***deleted***	*Tentative agreement in trilogue:* 4. Without prejudice to Articles 77 and 79, if a processor in breach of this regulation determines the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.	***deleted***	***deleted***	

Article 27	***Article 27***	***Article 27***	***Article 27***
Processing under the authority of the controller and processor	***Processing under the authority of the controller and processor***	***Processing under the authority of the controller and processor***	***Processing under the authority of the controller and processor***
The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	***deleted***	*Tentative agreement in trilogue:* The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.
Article 28	***Article 28***	***Article 28***	***Article 28***
Documentation	***Documentation***	***Records of categories of personal data processing activities***	***Records of processing activities***
	Amendment 122		
1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	1. Each controller and processor ~~and, if any, the controller's representative,~~ shall maintain ***regularly updated*** documentation ~~of all processing operations under its responsibility~~ ***necessary to fulfill the requirements laid down in this Regulation***.	1. Each controller ~~and processor~~ and, if any, the controller's representative, shall maintain ***a record*** ~~documentation~~ of all ***categories of personal data*** processing ~~operations~~ ***activities*** under its responsibility. ~~The documentation~~ ***This record*** shall contain ~~at least~~ the following information:	*Tentative agreement in trilogue:* 1. Each controller and, if any, the controller's representative, shall maintain a record of processing activities under its responsibility. This record shall contain the following information:

2. The documentation shall contain at least the following information:	2. ~~The~~ ***In addition, each controller and processor shall maintain*** documentation ~~shall contain at least~~ ***of*** the following information:	***[Merged with 1. above and slightly modified]***	
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller~~, or~~ ***and*** any joint controller ~~or processor~~, ~~and of the~~***controller's*** representative ***and data protection officer***, if any;	*Tentative agreement in trilogue:* (a) the name and contact details of the controller and any joint controller, the controller's representative and the data protection officer, if any;
(b) the name and contact details of the data protection officer, if any;	(b) the name and contact details of the data protection officer, if any;	***deleted***	
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	***deleted***	(c) the purposes of the processing, including the legitimate interests~~ pursued by the controller where~~***when*** the processing is based on ~~point (f) of~~ Article 6(1)***(f)***;	*Tentative agreement in trilogue:* (c) the purposes of the processing;
(d) a description of categories of data subjects and of the categories of personal data relating to them;	***deleted***	(d) a description of categories of data subjects and of the categories of personal data relating to them;	*Tentative agreement in trilogue:* (d) a description of categories of data subjects and of the categories of personal data;
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;	(e) the ~~recipients or categories of recipients of the personal data, including~~ ***name and contact details of*** the controllers to whom personal data are disclosed ~~for the legitimate interest pursued by them~~***, if any***;	(e) the ~~recipients or~~ categories of recipients ~~of~~ ***to whom*** the personal data~~, including the controllers to whom personal data are~~ ***have been or will be*** disclosed~~ for the legitimate interest pursued by them~~ ***in particular recipients in third countries***;	*Tentative agreement in trilogue:* (e) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries;

(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	***deleted***	(f) where applicable, ***the categories of*** transfers of ***personal*** data to a third country or an international organisation~~, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards~~;	*Tentative agreement in trilogue :* (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
(g) a general indication of the time limits for erasure of the different categories of data;	***deleted***	(g) ***where possible, the envisaged*** ~~a general indication of the~~ time limits for erasure of the different categories of data;	*Tentative agreement in trilogue:* (g) where possible, the envisaged time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).	***deleted***	(h) ***where possible, a general description of the technical and organisational security measures*** ~~the description of the mechanisms~~ referred to in Article ~~22~~***30***(~~3~~***1***).	*Tentative agreement in trilogue:* (h) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).
		2a. Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:	*Tentative agreement in trilogue:* 2a. Each processor and, if any, the processor's representative shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:

		(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;	*Tentative agreement in trilogue:* (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's or the processor's representative, and the data protection officer, if any;
		(b) the name and contact details of the data protection officer, if any;	
		(c) the categories of processing carried out on behalf of each controller;	*Tentative agreement in trilogue:* (c) the categories of processing carried out on behalf of each controller;
		(d) where applicable, the categories of transfers of personal data to a third country or an international organisation;	*Tentative agreement in trilogue:* (d) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

		(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).	*Tentative agreement in trilogue:* (e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).
		3a. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic or other non-legible form which is capable of being converted into a legible form.	*Tentative agreement in trilogue:* 3a. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic form.
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	***deleted***	3. ***On request,*** ~~T~~*t*he controller and the processor and, if any, the controller's representative, shall make the ~~documentation~~ ***record*** available~~, on request,~~ to the supervisory authority.	*Tentative agreement in trilogue:* 3. Upon request, the controller and the processor and, if any, the controller's or the processor's representative, shall make the record available to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:	***deleted***	4. The obligations referred to in paragraphs 1 and 2***a*** shall not apply to~~ the following controllers and processors~~:	*Presidency suggestion:* 4. The obligations referred to in paragraphs 1 and 2a shall not apply to
(a) a natural person processing personal data without a commercial interest; or	***deleted***	(a) ~~a natural person processing personal data without a commercial interest; or~~	

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	***deleted***	(b) an enterprise or an organisation employing fewer than 250 persons ~~that is~~ ***unless the*** processing ~~personal data only as an activity ancillary to its main activities~~ ***it carries out is likely to result in a high risk for the rights and freedoms of data subject such as discrimination, identity theft or fraud, unauthorized reversal of pseudonymisation, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing.***	*Presidency suggestion:* (b) an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk for the rights and freedoms of data subject, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or processing of data relating to criminal convictions and offences referred to in Article 9a.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.	***deleted***	***deleted***	

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	
Article 29	***Article 29***	***Article 29***	***Article 29***
Co-operation with the supervisory authority	***Co-operation with the supervisory authority***	***Co-operation with the supervisory authority***	***Co-operation with the supervisory authority***
	Amendment 123		
1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	1. The controller and***, if any,*** the processor and~~, if any,~~ the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	***deleted***	*Tentative agreement in trilogue:* 1. The controller and the processor and, if any, the representative of the controller or the processor, shall co-operate, on request, with the supervisory authority in the performance of its tasks.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	***deleted***	

SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY
Article 30	***Article 30***	***Article 30***	***Article 30***
Security of processing	***Security of processing***	***Security of processing***	***Security of processing***
	Amendment 124		
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing ~~and the nature of the personal data to be protected~~, ***taking into account the results of a data protection impact assessment pursuant to Article 33,*** having regard to the state of the art and the costs of their implementation.	1. ***Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals,*** ~~T~~***t***he controller and the processor shall implement appropriate technical and organisational measures***, such as pseudonymisation of personal data*** to ensure a level of security appropriate to the risk~~s represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation~~.	*Presidency suggestion:* 1. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures***,*** to ensure a level of security appropriate to the risk, including inter alia, as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (c) the ability to restore the

			availability and access to data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
	1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include:	***1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.***	*Tentative agreement in trilogue:* 1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
	(a) the ability to ensure that the integrity of the personal data is validated;		
	(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;		

	(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;		
	(d) in the case of sensitive personal data processing according to Articles 8 and 9, additional security measures to ensure situational awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data;		
	(e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.		

2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.	2. The ~~controller and the processor shall, following an evaluation of the risks, take the~~ measures referred to in paragraph 1 ~~to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.~~ ***shall at least:***	***deleted***	
	(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;		
	(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and		
	(c) ensure the implementation of a security policy with respect to the processing of personal data.		

		2a. 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 requirements set out in paragraph 1.	*Presidency suggestion:* 2a. Adherence to an approved code 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 requirements set out in paragraph 1.
		2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	*Tentative agreement in trilogue:* 2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.	3. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions~~ ***entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default~~, unless paragraph 4 applies~~.	***deleted***	
4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:	***deleted***	***deleted***	
(a) prevent any unauthorised access to personal data;	***deleted***	***deleted***	

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;	***deleted***	***deleted***	
(c) ensure the verification of the lawfulness of processing operations.	***deleted***	***deleted***	
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

Article 31	*Article 31*	*Article 31*	*Article 31*
Notification of a personal data breach to the supervisory authority	***Notification of a personal data breach to the supervisory authority***	***Notification of a personal data breach to the supervisory authority***	***Notification of a personal data breach to the supervisory authority***
	Amendment 125		
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.	1. In the case of a personal data breach, the controller shall without undue delay ~~and, where feasible, not later than 24 hours after having become aware of it,~~ notify the personal data breach to the supervisory authority. ~~The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours~~.	1. In the case of a personal data breach ***which is likely to result in a high risk for the rights and freedoms of individuals, such as 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 significant economic or social disadvantage***, the controller shall without undue delay and, where feasible, not later than ~~24~~ ***72*** hours after having become aware of it, notify the personal data breach to the supervisory authority ***competent in accordance with Article 51***. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within ~~24~~ ***72*** hours.	*Presidency suggestion:* 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51, unless the controller is able to demonstrate that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

		1a. The notification referred to in paragraph 1 shall not be required if a communication to the data subject is not required under Article 32(3)(a) and (b).	*Presidency suggestion: deleted*
2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.	2. ~~Pursuant to point (f) of Article 26(2), the~~ ***The*** processor shall alert and inform the controller ~~immediately~~ ***without undue delay*** after the establishment of a personal data breach.	2. ~~Pursuant to point (f) of Article 26(2),~~ ~~t~~***T***he processor shall ~~alert~~***notify*** ~~and inform~~ the controller ~~immediately after the establishment~~ ***without undue delay after becoming award*** of a personal data breach.	*Tentative agreement in trilogue:* 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 must at least:	3. The notification referred to in paragraph 1 must at least:	3. The notification referred to in paragraph 1 must at least:	*Tentative agreement in trilogue:* 3. The notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including ***where possible and appropriate,*** the ***approximate*** categories and number of data subjects concerned and the categories and ***approximate*** number of data records concerned;	*Tentative agreement in trilogue:* (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	*Tentative agreement in trilogue:* (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	***deleted***	
(d) describe the consequences of the personal data breach;	(d) describe the consequences of the personal data breach;	(d) describe the ***likely*** consequences of the personal data breach ***identified by the controller***;	*Tentative agreement in trilogue:* (d) describe the likely consequences of the personal data breach;
(e) describe the measures proposed or taken by the controller to address the personal data breach.	(e) describe the measures proposed or taken by the controller to address the personal data breach ***and/or mitigate its effects***. ***The information may if necessary be provided in phases.***	(e) describe the measures ***taken or*** proposed ~~or~~ ***to be*** taken by the controller to address the personal data breach~~.~~; ***and***	*Tentative agreement in trilogue:* (e) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.
		(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.	
		3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.	*Tentative agreement in trilogue:* 3a. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must ***be sufficient to*** enable the supervisory authority to verify compliance with this Article ***and with Article 30***. The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches ***referred to in paragraphs 1 and 2***, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. ~~The documentation shall only include the information necessary for that purpose.~~	*Tentative agerement in trilogue:* 4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article.
	4a. The supervisory authority shall keep a public register of the types of breaches notified.		
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.	**5.** The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~ ***entrusted with the task*** of ~~further specifying the criteria and requirements~~ ***issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** for establishing the data breach ***and determining the undue delay*** referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor ~~is~~***are*** required to notify the personal data breach.	***deleted***	

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

Article 32	*Article 32*	*Article 32*	*Article 32*
Communication of a personal data breach to the data subject	***Communication of a personal data breach to the data subject***	***Communication of a personal data breach to the data subject***	***Communication of a personal data breach to the data subject***
	Amendment 126		
1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. When the personal data breach is likely to adversely affect the protection of the personal data***, the*** ~~or~~ privacy***, the rights or the legitimate interests*** of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. When the personal data breach is likely to ~~adversely affect the protection of the personal data or privacy of the data subject~~ ***result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage***, the controller shall~~, after the notification referred to in Article 31,~~ communicate the personal data breach to the data subject without undue delay.	*Presidency suggestion:* 1. When the personal data breach is likely to result in a high risk for the rights and freedoms of individuals the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).	2. The communication to the data subject referred to in paragraph 1 shall ***be comprehensive and use clear and plain language. It shall*** describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) ~~and~~***,*** (c) ***and (d)*** of Article 31(3) ***and information about the rights of the data subject, including redress.***	2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b)***, (e)*** and (~~e~~***f***) of Article 31(3).	*Tentative agreement in trilogue:* 2. The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b)***,*** (d) and (e) of Article 31(3).
3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3. The communication ~~of a personal data breach~~ to the data subject ***referred to in paragraph 1*** shall not be required if***:*** ***a.*** the controller ~~demonstrates to the satisfaction of the supervisory authority that it~~ has implemented appropriate technological ***and organisational*** protection measures, and that those measures were applied to the data ~~concerned~~***affected*** by the personal data breach***, in particular those that*** ~~.Such technological protection measures shall~~ render the data unintelligible to any person who is not authorised to access it***, such as encryption;or***	*Tentative agreement in trilogue:* 3. The communication to the data subject referred to in paragraph 1 shall not be required if: a. the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption;or

		b. the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or ***c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or*** ***d. it would adversely affect a substantial public interest.***	b. the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or c. it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or [d. it would adversely affect a substantial public interest.]
4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	***deleted***	*Tentative agreement in trilogue:* 4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.	5. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~ ***entrusted with the task*** of ~~further specifying the criteria and requirements~~ ***issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** as to the circumstances in which a personal data breach is likely to adversely affect the personal data***, the privacy, the rights or the legitimate interests of the data subject*** referred to in paragraph 1.	***deleted***	
6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

	Amendment 127		
	Article 32a		
	Respect to Risk		
	1. The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks.		
	2. The following processing operations are likely to present specific risks:		
	(a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;		
	(b) processing of 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;		

	(c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;		
	(d) processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;		
	(e) automated monitoring of publicly accessible areas on a large scale;		
	(f) other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);		
	(g) where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;		

	(h) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects;		
	(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.		
	3. According to the result of the risk analysis:		
	(a) where any of the processing operations referred to in points (a) or (b) of paragraph 2 exist, controllers not established in the Union shall designate a representative in the Union in line with the requirements and exemptions laid down in Article 25;		
	(b) where any of the processing operations referred to in points (a), (b) or (h)of paragraph 2 exist, the controller shall designate a data protection officer in line with the requirements and exemptions laid down in Article 35;		

	(c) where any of the processing operations referred to in points (a), (b), (c), (d), (e), (f), (g) or (h) of paragraph 2 exist, the controller or the processor acting on the controller's behalf shall carry out a data protection impact assessment pursuant to Article 33;		
	(d) where processing operations referred to in point (f) of paragraph 2 exist, the controller shall consult the data protection officer, or in case a data protection officer has not been appointed, the supervisory authority pursuant to Article 34.		
	4. The risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly. Where pursuant to point (c) of paragraph 3 the controller is not obliged to carry out a data protection impact assessment, the risk analysis shall be documented.		

SECTION 3 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION	SECTION 3 *LIFECYCLE* DATA PROTECTION *MANAGEMENT*	SECTION 3 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION	SECTION 3 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR AUTHORISATION
Article 33	~~***Article 33***~~	~~***Article 33***~~	***Article 33***
Data protection impact assessment	~~***Data protection impact assessment***~~	~~***Data protection impact assessment***~~	***Data protection impact assessment***
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	1. Where ~~processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,~~ ***required pursuant to point (c) of Article 32a(3)*** the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the ***rights and freedoms of the data subjects, especially their right to*** protection of personal data. ***A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.***	1. Where ***a type of*** processing ***in particular using new technologies, and taking into account*** ~~operations present specific risks to the rights and freedoms of data subjects by virtue of their~~ ***the*** nature, ~~their~~ ***scope, context and*** ~~***or***~~ ~~their~~ purposes ***of the processing, is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorised reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller or the processor acting on the controller's behalf shall,***	*Tentative agreement in trilogue:* 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

		prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	
		1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.	*Tentative agreement in trilogue:* 1a. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
2. The following processing operations in particular present specific risks referred to in paragraph 1:	***deleted***	2. ~~The following processing operations in particular present specific risks~~ ***A data protection impact assessment*** referred to in paragraph 1 ***shall in particular be required in the following cases***:	*Tentative agreement in trilogue:* 2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the following cases:

(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;	***Deleted***	(a) a systematic and extensive evaluation of personal aspects relating to ~~a~~ natural person***s*** ~~or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing~~ ***which is based on profiling*** and on which ~~measures~~ ***decisions*** are based that produce legal effects concerning ~~the individual~~ ***data subjects*** or ~~significantly~~ ***severely*** affect ~~the individual~~***data subjects***;	*Tentative agreement in trilogue:* (a) a systematic and extensive evaluation of personal aspects relating to natural person***s*** which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual;
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;	***Deleted***	(b) ~~information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases~~ ***processing of special categories of personal data under Article 9(1), biometric data or data on criminal convictions and offences or related security measures***, where the data are processed for taking ~~measures or~~ decisions regarding specific individuals on a large scale;	*Tentative agreement in trilogue:* (b) processing on a large scale of special categories of data referred to in Article 9(1), of data relating to criminal convictions and offences referred to in Article 9a, or of biometric data;

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;	***Deleted***	(c) monitoring publicly accessible areas **on a large scale**, especially when using optic-electronic devices ~~(video surveillance) on a large scale~~;	*Tentative agreement in trilogue:* (c) a sytematic monitoring of a publicly accessible area on a large scale
(d) personal data in large scale filing systems on children, genetic data or biometric data;	***deleted***	***deleted***	
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).	***deleted***	***deleted***	
2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists and any updates to the European Data Protection Board.		***2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board.***	*Tentative agreement in trilogue:* 2a. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board.

		2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.	*Tentative agreement in trilogue:* 2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.
		2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.	*Tentative agreement in trilogue:* 2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.	3. The assessment shall ***have regard to the entire lifecycle management of personal data from collection to processing to deletion. It shall*** contain at least ~~a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned~~***:***	3. The assessment shall contain at least a general description of the envisaged processing operations, an ~~assessment~~ ***evaluation*** of the risk~~s to the rights and freedoms of data subjects~~ ***referred to in paragraph 1***, the measures envisaged to address the risk~~s,~~ ***including*** safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.	*Tentative agreement in trilogue:* 3. The assessment shall contain at least:
	(a) a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller;		*Tentative agreement in trilogue:* (a) a systematic description of the envisaged processing operations, the purposes of the processing, including where applicable the legitimate interest pursued by the controller;
	(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;		*Tentative agreement in trilogue:* (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

	(c) an assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation;		*Tentative agreement in trilogue:* c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;
	(d) a description of the measures envisaged to address the risks and minimise the volume of personal data which is processed;		*Tentative agreement in trilogue:* (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
	(e) a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned;		
	(f) a general indication of the time limits for erasure of the different categories of data;		

	(g) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;		
	(h) a list of the recipients or categories of recipients of the personal data;		
	(i) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation ~~and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards~~;		
	(j) an assessment of the context of the data processing.		
	3a. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.		

	3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies. The controller and the processor and, if any, the controller's representative shall make the assessment available, on request, to the supervisory authority.		
		3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.	*Presidency suggestion:* 3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	***deleted***	4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	*Tentative agreement in trilogue:* 4. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.	***deleted***	5. Where ~~the controller is a public authority or body and where~~ the processing ~~results from a legal obligation~~ pursuant to point (c) ***or (e)*** of Article 6(1) ~~providing for rules and procedures pertaining to the processing operations and regulated by~~ ***has a legal basis in*** Union law~~, paragraphs 1 to 4 shall not apply, unless~~ ***or the law of the*** Member State~~s~~ ***to which the controller is subject, and such law regulates the specific processing operation or set of operations in question, paragraphs 1 to 3 shall not apply, unless Member States*** deem it necessary to carry out such assessment prior to the processing activities.	*Presidency suggestion:* 5. Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law, or the law of the Member State~~s~~ to which the controller is subject, and such law regulates the specific processing operation or set of operations in question, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	***deleted***	***deleted***	
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

			Tentative agreement in trilogue: 8. Where necessary, the controller shall carry out a review to assess if the processing of personal data is performed in compliance with the data protection impact assessment at least when there is a change of the risk represented by the processing operations.
	Amendment 130		
	Article 33 a (new)		
	Data protection compliance review		
	1. At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment.		

	2. The compliance review shall be carried out periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations.		
	3. Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance.		
	4. The compliance review and its recommendations shall be documented. The controller and the processor and, if any, the controller's representative shall make the compliance review available, on request, to the supervisory authority.		
	5. If the controller or the processor has designated a data protection officer, he or she shall be involved in the compliance review proceeding.		

Article 34	*Article 34*	*Article 34*	*Article 34*
	Amendment 131		
Prior authorisation and prior consultation	***Prior consultation***	**Prior ~~authorisation and prior~~ consultation**	**Prior consultation**
1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.	***deleted***	***deleted***	

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:	2. The controller or processor acting on the controller's behalf shall consult the ***data protection officer, or in case a data protection officer has not been appointed, the*** supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:	2. The controller ~~or processor acting on the controller's behalf~~ shall consult the supervisory authority prior to the processing of personal data ***where a data protection impact assessment as provided for in Article 33 indicates that the*** ~~in order to ensure the compliance of the intended~~ processing ~~with this Regulation and in particular to mitigate the~~ ***would result in a high*** risk~~s involved for the data subjects where:~~***in the absence of measures to be taken by the controller to mitigate the risk.***	*Tentative agreement in trilogue:* 2. The controller shall consult, the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or	(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or	***deleted***	
(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	(b) ***the data protection officer or*** the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	***deleted***	

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.	3. Where the ***competent*** supervisory authority ~~is of the opinion~~ ***determines in accordance with its power*** that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.	3. Where the supervisory authority is of the opinion that the intended processing ***referred to in paragraph 2 would*** ~~does~~ not comply with this Regulation, in particular where ***the controller has*** ~~risks are~~ insufficiently identified or mitigated **the risk**, it shall ~~prohibit the intended processing and make appropriate proposals to remedy such incompliance~~ ***within a maximum period of 6 weeks following the request for consultation give advice to the data controller , in writing, and may use any of its powers referred to in Article 53. This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.***	*Tentative agreement in trilogue:* 3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, it shall within a maximum period of eight weeks following the request for consultation give advice to the data controller, and where applicable the processor in writing, and may use any of its powers referred to in Article 53. This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller, and where applicable the processor shall be informed within one month of receipt of the request including of the reasons for the delay. These periods may be suspended until the supervisory authority has obtained any information it may have requested for the purposes of the consultation.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	4. The ~~supervisory authority~~ ***European Data Protection Board*** shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to ~~point (b) of~~ paragraph 2. ~~The supervisory authority shall communicate those lists to the European Data Protection Board~~.	***deleted***	
5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.	***deleted***	***deleted***	

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	6. The controller or processor shall provide the supervisory authority***, on request,*** with the data protection impact assessment ~~provided for in~~ ***pursuant to*** Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	6. ***When consulting the supervisory authority pursuant to paragraph2,*** ~~T~~***t***he controller ~~or processor~~ shall provide the supervisory authority***,*** with ***(a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;*** ***(b) the purposes and means of the intended processing;*** ***(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;*** ***(d) where applicable, the contact details of the data protection officer;*** ***(e)*** the data protection impact assessment provided for in Article 33***;*** and ***(f)***~~, on request, with~~ any other information ~~to allow~~ ***requested by*** the supervisory authority ~~to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards~~.	*Tentative agreement in trilogue:* 6. When consulting the supervisory authority pursuant to paragraph2, the controller shall provide the supervisory authority, with (a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings; (b) the purposes and means of the intended processing; (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation; (d) where applicable, the contact details of the data protection officer; (e) the data protection impact assessment provided for in Article 33; and (f) any other information requested by the supervisory authority.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority ~~in~~ ***during*** the preparation of a ***proposal for a*** legislative measure ~~to be~~ adopted by ~~the~~***a*** national parliament or of a ***regulatory*** measure based on such a legislative measure***,*** which ~~defines the nature of the processing, in order to ensure the compliance of the intended~~ ***provide for the*** processing ~~with this Regulation and in particular to mitigate the risks involved for the data subjects~~ ***of personal data***.	*Tentative agreement in trilogue:* 7. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regultory measure based on such a legislative measure, which relates to the processing of personal data.
		7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.	*Tentative agreement in trilogue:* 7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.	***deleted***	***deleted***	
9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***deleted***	***deleted***	

SECTION 4 DATA PROTECTION OFFICER	SECTION 4 DATA PROTECTION OFFICER	SECTION 4 DATA PROTECTION OFFICER	SECTION 4 DATA PROTECTION OFFICER
Article 35	***Article 35***	***Article 35***	***Article 35***
Designation of the data protection officer	***Designation of the data protection officer***	***Designation of the data protection officer***	***Designation of the data protection officer***
	Amendment 132		
1. The controller and the processor shall designate a data protection officer in any case where:	1. The controller and the processor shall designate a data protection officer in any case where :	1. The controller ~~and~~ ***or*** the processor ***may, or where required by Union or Member State law*** shall designate a data protection officer ~~in any case where:~~**.**	*Presidency suggestion:* 1. The controller and the processor shall designate a data protection officer in any case where :
(a) the processing is carried out by a public authority or body; or	(a) the processing is carried out by a public authority or body; or	***deleted***	*Presidency suggestion:* a) the processing is carried out by a public authority or body; or
(b) the processing is carried out by an enterprise employing 250 persons or more; or	(b) the processing is carried out by ~~an enterprise employing 250 persons or more~~ ***a legal person and relates to more than 5000 data subjects in any consecutive 12-month period***; or	***deleted***	

(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects***; or***	***deleted***	*Presidency suggestion:* (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of the data subjects; or
	(d) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems.		*Presidency suggestion:* (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and data relating to criminal convictions and offences referred to in Article 9a.
2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	2. ~~In the case referred to in point (b) of paragraph 1, a~~ ***A*** group of undertakings may appoint a ~~single~~ ***main responsible*** data protection officer***, provided it is ensured that a data protection officer is easily accessible from each establishment.***	2. ~~In the case referred to in point (b) of paragraph 1, a~~ ***A*** group of undertakings may appoint a single data protection officer.	*Presidency suggestion:* 2. A group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.	3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.	3. Where the controller or the processor is a public authority or body, ~~the~~ ***a single*** data protection officer may be designated for several ~~of its entities~~ ***such authorities or bodies***, taking account of the***ir*** organisational structure ~~of the public authority or body~~ ***and size***.	*Tentative agreement in trilogue:* 3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	***deleted***	*Presidency suggestion:* 4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	5. The ~~controller or processor shall designate the~~ data protection officer ***shall be designated*** on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37***, particularly the absence of any conflict of interests***. ~~The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.~~	*Tentative agreement in trilogue:* 5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37, particularly the absence of any conflict of interests.
6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	***deleted***	

7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.	7. The controller or the processor shall designate a data protection officer for a period of at least ~~two~~ ***four*** years ***in case of an employee or two years in case of an external service contractor***. The data protection officer may be reappointed for further terms. During ~~their~~ ***his or her*** term of office, the data protection officer may only be dismissed, if ~~the data protection officer~~ ***he or she*** no longer fulfils the conditions required for the performance of ~~their~~ ***his or her*** duties.	7. ~~The controller or the processor shall designate a~~ ***During their term of office, the*** data protection officer ~~for a period of at least two years. The data protection officer~~ may***, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant,*** ~~be reappointed for further terms. During their term of office, the data protection officer may only~~ be dismissed~~,~~ ***only*** if the data protection officer no longer fulfils the conditions required for the performance of ~~their duties~~ ***his or her tasks pursuant to Article 37***.	*Presidency suggestion:* 7. During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her tasks pursuant to Article 37.
8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8. The data protection officer may be ~~employed by~~ ***a staff member of*** the controller or processor, or fulfil ~~his or her~~ ***the*** tasks on the basis of a service contract.	*Tentative agreement in trilogue:* 8. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	9. The controller or the processor shall ~~communicate~~ ***publish*** the ~~name and~~ contact details of the data protection officer ***and communicate these*** to the supervisory authority ~~and to the public~~.	*Tentative agreement in trilogue:* 9. The controller or the processor shall publish the contact details of the data protection officer and communicate these to the supervisory authority.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects ~~shall have the right to~~ ***may*** contact the data protection officer on all issues related to the processing of the data subject's data and ~~to request exercising the~~ ***the exercise of their*** rights under this Regulation.	*Moved to Article 36(2a new)*
11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.	***deleted***	***deleted***	

Article 36	*Article 36*	*Article 36*	*Article 36*
Position of the data protection officer	***Position of the data protection officer***	***Position of the data protection officer***	***Position of the data protection officer***
	Amendment 133		
1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	*Tentative agreement in trilogue:* 1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.
2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.	2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the ***executive*** management of the controller or the processor. ***The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation***.	2. The controller or processor shall ~~ensure that~~ ***support*** the data protection officer ***in*** perform~~s~~***ing*** the ~~duties and~~ tasks ***referred to in Article 37 by providing resources necessary to carry out these tasks as well as access to personal data and processing operations*** ~~independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor~~.	*Tentative agreement in trilogue:* 2. The controller or processor shall support the data protection officer in performing the tasks referred to in Article 37 by providing resources necessary to carry out these tasks as well as access to personal data and processing operations, and to maintain his or her expert knowledge.

			Tentative agreement in trilogue: (2a new) Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation.
3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.	3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide ***all means, including*** staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37***, and to maintain his or her professional knowledge***.	3. The controller or ~~the~~ processor shall ~~support~~ ***ensure that*** the data protection officer ***can act*** in ***an independent manner with respect to the*** perform~~ing~~***ance of his or her*** ~~the~~ tasks ~~and shall provide staff, premises, equipment and any other resources necessary to carry out the duties~~ and ***does not receive any instructions regarding the exercise of these*** tasks~~ referred to in Article 37~~***. He or she shall not be penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.***	*Tentative agreement in trilogue:* 3. The controller or processor shall ensure that the data protection officer can act in an independent manner with respect to the performance of his or her tasks and does not receive any instructions regarding the exercise of these tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

	4. Data protection officers shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from that obligation by the data subject.		*Tentative agreement in trilogue:* 4. Data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
		4. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.	*Tentative agreement in trilogue:* 4a. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 37	***Article 37***	***Article 37***	***Article 37***
Tasks of the data protection officer	***Tasks of the data protection officer***	***Tasks of the data protection officer***	***Tasks of the data protection officer***
	Amendment 134		
1. The controller or the processor shall entrust the data protection officer at least with the following tasks:	~~1.~~ The controller or the processor shall entrust the data protection officer at least with the following tasks:	1. The ~~controller or the processor shall entrust the~~ data protection officer ~~at least with~~ ***shall have*** the following tasks:	*Tentative agreement in trilogue:* 1. The data protection officer shall have at least the following tasks:
(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;	(a) ***to raise awareness,*** to inform and advise the controller or the processor of their obligations pursuant to this Regulation***, in particular with regard to technical and organisational measures and procedures,*** and to document this activity and the responses received;	(a) to inform and advise the controller or the processor ***and the employees who are processing personal data*** of their obligations pursuant to this Regulation and ~~to document this activity and the responses received~~ ***other Union or Member State data protection provisions***;	*Tentative agreement in trilogue:* (a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;	(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;	(b) to monitor ***compliance with this Regulation, with other Union or Member State data protection provisions and with*** the ~~implementation and application of the~~ policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, ***awareness-raising and*** ~~the~~ training of staff involved in the processing operations, and the related audits;	*Tentative agreement in trilogue:* (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;

(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	***deleted***	
(d) to ensure that the documentation referred to in Article 28 is maintained;	(d) to ensure that the documentation ~~referred~~ to in ~~Article~~ 28 is maintained;	***deleted***	
(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;	(e) to monitor the documentation, notification and communication of personal data breaches pursuant to ~~Articles~~ 31 and 32;	***deleted***	
(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;	(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior ~~authorisation or prior~~ consultation, if required pursuant ***to*** Articles ***32a,*** 33 and 34;	(f) to ~~monitor the performance of~~ ***provide advice where requested as regards*** the data protection impact assessment ~~by the controller or processor~~ and ~~the application for prior authorisation or prior consultation, if required~~ ***monitor its performance*** pursuant Article~~s~~ 33 ~~and 34~~;	*Tentative agreement in trilogue:* (f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;	(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;	(g) to monitor ~~the~~ response***s*** to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, ***to*** co-~~operating~~***operate*** with the supervisory authority at the latter's request or on the data protection officer's own initiative;	*Tentative agreement in trilogue:* (g) to monitor responses to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, to cooperate with the supervisory authority at the latter's request or on the data protection officer's own initiative;
(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.	(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative**.**	(h) to act as the contact point for the supervisory authority on issues related to the processing ***of personal data, including the prior*** ~~*and*~~ consult***ation referred to in Article 34, and consult, as*** ~~with the supervisory authority, if~~ appropriate, on ~~his/her own initiative~~ ***any other matter***.	*Tentative agreement in trilogue:* (h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter.
	(i) to verify the compliance with this Regulation under the prior consultation mechanism laid out in Article 34;		
	(j) to inform the employee representatives on data processing of the employees.		

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.	***deleted***	***deleted***	
		2a. The data protection officer shall in the performance his or her tasks have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.	*Tentative agreement in trilogue:* 2a. The data protection officer shall in the performance his or her tasks have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

SECTION 5 CODES OF CONDUCT AND CERTIFICATION	SECTION 5 CODES OF CONDUCT AND CERTIFICATION	SECTION 5 CODES OF CONDUCT AND CERTIFICATION	SECTION 5 CODES OF CONDUCT AND CERTIFICATION
Article 38	***Article 38***	***Article 38***	***Article 38***
Codes of conduct	***Codes of conduct***	***Codes of conduct***	***Codes of conduct***
	Amendment 135		
1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:	1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct ***or the adoption of codes of conduct drawn up by a supervisory authority*** intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:	1. The Member States, the supervisory authorities***, the European Data Protection Board*** and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors~~, in particular in relation to:~~ ***and the specific needs of micro, small and medium-sized enterprises.***	*Tentative agreement in trilogue:* 1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises.

		1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:	*Tentative agreement in trilogue:* 1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:
(a) fair and transparent data processing;	(a) fair and transparent data processing;	(a) fair and transparent data processing;	*Tentative agreement in trilogue:* (a) fair and transparent data processing;
	(aa) respect for consumer rights;		
		(aa) the legitimate interests pursued by controllers in specific contexts;	*Tentative agreement in trilogue:* (aa) the legitimate interests pursued by controllers in specific contexts;
(b) the collection of data;	(b) the collection of data;	(b) the collection of data;	*Tentative agreement in trilogue:* (b) the collection of data;
		(bb) the pseudonymisation of personal data;	*Tentative agreement in trilogue:* (bb) the pseudonymisation of personal data;
(c) the information of the public and of data subjects;	(c) the information of the public and of data subjects;	(c) the information of the public and of data subjects;	*Tentative agreement in trilogue:* (c) the information of the public and of data subjects;

(d) requests of data subjects in exercise of their rights;	(d) requests of data subjects in exercise of their rights;	(d) ~~requests of data subjects in~~***the*** exercise of the~~ir~~ rights ***of data subjects***;	*Tentative agreement in trilogue:* (d) the exercise of the rights of data subjects;
(e) information and protection of children;	(e) information and protection of children;	(e) information and protection of children ***and the way to collect the parent's and guardian's consent***;	*Tentative agreement in trilogue:* (e) information and protection of children and the way to collect the parent's and guardian's consent;
		(ee) measures and procedures referred to in Articles 22 and 23 and measures to ensure security of processing referred to in Article 30;	*Tentative agreement in trilogue:* (ee) measures and procedures referred to in Articles 22 and 23 and measures to ensure security of processing referred to in Article 30;
		(ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;	*Tentative agreement in trilogue:* (ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;
(f) transfer of data to third countries or international organisations;	(f) transfer of data to third countries or international organisations;	***deleted***	*Tentative agreement in trilogue:* (f) transfer of data to third countries or international organisations;
(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;	(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;	***deleted***	

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.	(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.	***deleted***	*Tentative agreement in trilogue:* (h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.
		1ab. In addition to adherence by controller or processor subject to the regulation, codes of conduct approved pursuant to paragraph 2 may also be adhered to by controllers or processors that are not subject to this Regulation according to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(d). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards including as regards data subjects' rights.	*Presidency suggestion:* 1ab. In addition to adherence by controller or processor subject to the regulation, codes of conduct approved pursuant to paragraph 2 may also be adhered to by controllers or processors that are not subject to this Regulation according to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(d). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards including as regards data subjects' rights.

		1b. Such a code of conduct shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.	*Tentative agreement in trilogue:* 1b. Such a code of conduct pursuant to paragraph 1a shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.	2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority ~~may~~ ***shall without undue delay*** give an opinion ***on*** whether ***the processing under*** the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.	2. Associations and other bodies ***referred to in paragraph 1a*** ~~representing categories of controllers or processors in one Member State~~ which intend to ~~draw up~~ ***prepare a*** code~~s~~ of conduct or to amend or extend an existing code~~s~~***,*** ~~of conduct may~~ ***shall*** submit the~~m to an opinion of~~ ***draft code to*** the supervisory authority ~~in that Member State~~ ***which is competent pursuant to Article 51***. The supervisory authority ~~may~~ ***shall*** give an opinion ***on*** whether the draft code***, or amended or extended code*** ~~of conduct or the amendment~~ is in compliance with this Regulation ***and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards***. ~~The supervisory authority shall seek the views of data subjects or their representatives on these drafts.~~	*Tentative agreement in trilogue:* 2. Associations and other bodies referred to in paragraph 1a which intend to prepare a code of conduct or to amend or extend an existing code, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code is in compliance with this Regulation and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards.

		2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code is approved, and if the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof.	*Tentative agreement in trilogue:* 2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code is approved, and if the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.
		2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.	*Tentative agreement in trilogue:* 2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.	3. Associations and other bodies representing categories of controllers ***or processors*** in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.	3. ~~Associations and other bodies representing categories of controllers in several Member States may submit draft~~ ***Where the opinion referred to in paragraph 2b confirms that the*** code~~s~~ of conduct***,*** ~~and~~ ***or*** amend~~ments~~***ed*** or extensions***ded*** ~~to existing~~ code~~s~~***,*** ~~of conduct to the Commission~~ ***is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards, the European Data Protection Board shall submit its opinion to the Commission***.	*Tentative agreement in trilogue:* 3. Where the opinion referred to in paragraph 2b confirms that the codes of conduct, or amended or extended codes, is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards, the European Data Protection Board shall submit its opinion to the Commission.

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	4. The Commission ~~may adopt implementing acts~~ ***shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86*** for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 ***are in line with this Regulation and*** have general validity within the Union. Those ~~implementing acts~~ ***delegated acts*** shall ~~be adopted in accordance with the examination procedure set out in Article 87(2)~~ ***confer enforceable rights on data subjects.***	4. The Commission may adopt implementing acts for deciding that the ***approved*** codes of conduct and amendments or extensions to existing ***approved*** codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	*Tentative agreement in trilogue:* 4. The Commission may adopt implementing acts for deciding that the approved codes of conduct and amendments or extensions to existing approved codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).
5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.	5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.	5. The Commission shall ensure appropriate publicity for the ***approved*** codes which have been decided as having general validity in accordance with paragraph 4.	*Tentative agreement in trilogue:* 5. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 4.

		5a. The European Data Protection Board shall collect all approved codes of conduct and amendments thereto in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.	*Tentative agreement in trilogue:* 5a. The European Data Protection Board shall collect all approved codes of conduct and amendments thereto in a register and shall make them publicly available through any appropriate means.

		Article 38a	***Article 38a***
		Monitoring of approved codes of conduct	***Monitoring of approved codes of conduct***
		1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.	*Tentative agreement in trilogue:* 1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38, may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.
		2. A body referred to in paragraph 1 may be accredited for this purpose if:	*Tentative agreement in trilogue:* 2. A body referred to in paragraph 1 may be accredited for this purpose if:
		(a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;	*Tentative agreement in trilogue:* (a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

		(b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;	*Tentative agreement in trilogue:* (b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
		(c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;	*Tentative agreement in trilogue:* (c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;
		(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.	*Tentative agreement in trilogue:* (d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

		3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.	*Tentative agreement in trilogue:* 3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.
		4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.	*Tentative agreement in trilogue:* 4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body referred to in paragraph 1 shall, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

		5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.	*Tentative agreement in trilogue:* 5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.
		6. This article shall not apply to the processing of personal data carried out by public authorities and bodies.	*Tentative agreement in trilogue:* 6. This article shall not apply to the processing of personal data carried out by public authorities and bodies.

Article 39	***Article 39***	***Article 39***	***Article 39***
Certification	***Certification***	***Certification***	***Certification***
	Amendment 136		
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.	***deleted***	1. The Member States***, the European Data Protection Board*** and the Commission shall encourage, in particular at ~~European~~ ***Union*** level, the establishment of data protection certification mechanisms and of data protection seals and marks, ***for the purpose of demonstrating compliance with this Regulation of processing operations carried out*** ~~allowing data subjects to quickly assess the level of data protection provided~~ by controllers and processors. The ~~data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the~~ specific ~~features of the various sectors and different processing operations~~***needs of micro, small and medium-sized entreprises shall be taken into account***.	*Tentative agreement in trilogue:* 1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations carried out by controllers and processors. The specific needs of micro, small and medium-sized entreprises shall be taken into account.

		1a. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 2a may also be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation according to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards, including as regards data subjects' rights.	*Presidency suggestion:* 1a. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 2a may also be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation according to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in Article 42(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual instruments or otherwise, to apply those appropriate safeguards, including as regards data subjects' rights.

	1a. Any controller or processor may request any supervisory authority in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal		
	data is performed in compliance with this Regulation, in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights.		
	1b. The certification shall be voluntary, affordable, and available via a process that is transparent and not unduly burdensome.		*Tentative agreement in trilogue:* 1b. The certification shall be voluntary and available via a process that is transparent.
	1c. The supervisory authorities and the European Data Protection Board shall cooperate under the consistency mechanism pursuant to Article 57 to guarantee a harmonised data protection certification mechanism including harmonised fees within the Union.		

	1d. During the certification procedure, the supervisory authority~~-~~ies may accredit specialised third party auditors to carry out the auditing of the controller or the processor on their behalf. Third party auditors shall have sufficiently qualified staff, be impartial and free from any conflict of interests regarding their duties. Supervisory authorities shall revoke accreditation, if there are reasons to believe that the auditor does not fulfil its duties correctly. The final certification shall be provided by the supervisory authority.		
	1e. Supervisory authorities shall grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with this Regulation, the standardised data protection mark named "European Data Protection Seal".		

	1f. The "European Data Protection Seal" shall be valid for as long as the data processing operations of the certified controller or processor continue to fully comply with this Regulation.		
	1g. Notwithstanding paragraph 1f, the certification shall be valid for maximum five years.		
	1h. The European Data Protection Board shall establish a public electronic register in which all valid and invalid certificates which have been issued in the Member States can be viewed by the public.		
	1i. The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with this Regulation.		

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.	2. The Commission shall be empowered to adopt***, after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-governmental organisations,*** delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in ~~paragraph 1~~***paragraphs 1a to 1h***, including ***requirements for accreditation of auditors,*** conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries. ***Those delegated acts shall confer enforceable rights on data subjects***.	***[Moved and modified under Article 39a point 7]***	
		2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.	*Presidency suggestion:* 2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.

		2a. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority on the basis of the criteria approved by the competent supervisory authority or, pursuant to Article 57, the European Data Protection Board.	*Presidency suggestion:* 2a. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority on the basis of the criteria approved by the competent supervisory authority or, pursuant to Article 57, the European Data Protection Board. In the latter case, the criteria approved by the European Data Protection Board may result in a common certification, the European Data Protection Seal.
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	***deleted***	***deleted***	

		3. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 39a, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.	*Presidency suggestion:* 3. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 39a, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.
		4. The certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the relevant requirements continue to be met. It shall be withdrawn by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority where the requirements for the certification are not or no longer met.	*Presidency suggestion:* 4. The certification shall be issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions as long as the relevant requirements continue to be met. It shall be withdrawn by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority where the requirements for the certification are not or no longer met.

		5. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.	*Presidency suggestion:* 5. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means.

		Article 39a	***Article 39a***
		Certification body and procedure	***Certification body and procedure***
		1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification shall be issued and renewed by a certification body which has an appropriate level of expertise in relation to data protection. Each Member State shall provide whether these certification bodies are accredited by:	*Presidency suggestion:* 1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification shall be issued and renewed [after informing the supervisory authority] by a certification body which has an appropriate level of expertise in relation to data protection. Each Member State shall provide whether these certification bodies are accredited by:
		(a) the supervisory authority which is competent according to Article 51 or 51a; and/or	*Presidency suggestion:* (a) the supervisory authority which is competent according to Article 51 or 51a; and/or

		(b) the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent according to Article 51 or 51a.	*Presidency suggestion:* (b) the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European Parliament and the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products in compliance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent according to Article 51 or 51a.
		2. The certification body referred to in paragraph 1 may be accredited for this purpose only if:	*Presidency suggestion:* 2. The certification body referred to in paragraph 1 may be accredited for this purpose only if:
		(a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;	*Tentative agreement in trilogue:* (a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

		(aa) it has undertaken to respect the criteria referred to in paragraph 2a of Article 39 and approved by the supervisory authority which is competent according to Article 51 or 51a or , pursuant to Article 57, the European Data Protection Board;	*Tentative agreement in trilogue:* (aa) it has undertaken to respect the criteria referred to in paragraph 2a of Article 39 and approved by the supervisory authority which is competent according to Article 51 or 51a or, pursuant to Article 57, the European Data Protection Board;
		(b) it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;	*Tentative agreement in trilogue:* (b) it has established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
		(c) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;	*Tentative agreement in trilogue:* (c) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;

		(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.	*Tentative agreement in trilogue:* (d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.
		3. The accreditation of the certification bodies referred to in paragraph 1 shall take place on the basis of criteria approved by the supervisory authority which is competent according to Article 51 or 51a or, pursuant to Article 57, the European Data Protection Board. In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.	*Presidency suggestion:* 3. The accreditation of the certification bodies referred to in paragraph 1 shall take place on the basis of criteria approved by the supervisory authority which is competent according to Article 51 or 51a or, pursuant to Article 57, the European Data Protection Board. In case of an accreditation pursuant to point (b) of paragraph 1, these requirements complement those envisaged in Regulation 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

		4. The certification body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation is issued for a maximum period of five years and can be renewed in the same conditions as long as the body meets the requirements.	*Presidency suggestion:* 4. The certification body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation is issued for a maximum period of five years and can be renewed in the same conditions as long as the body meets the requirements.
		5. The certification body referred to in paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.	*Presidency suggestion:* 5. The certification body referred to in paragraph 1 shall provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification.

		6. The requirements referred to in paragraph 3 and the criteria referred to in paragraph 2a of Article 39 shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit these to the European Data Protection Board. ***The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.***	*Tentative agreement in trilogue:* 6. The requirements referred to in paragraph 3 and the criteria referred to in paragraph 2a of Article 39 shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit these to the European Data Protection Board. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means.
		6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority or the National Accreditation Body shall revoke the accreditation it granted to a certification body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.	*Presidency suggestion:* 6a. Without prejudice to the provisions of Chapter VIII, the competent supervisory authority or the National Accreditation Body shall revoke the accreditation it granted to a certification body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

		7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86, for the purpose of specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1 ~~including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries~~.	*Tentative agreement in trilogue:* 7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86, for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1 of Article 39.
		7a. The European Data Protection Board shall give an opinion to the Commission on the criteria and requirements referred to in paragraph 7.	*Move to Article 66*

	deleted	***8.*** The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)**.**	*Tentative agreement in trilogue:* 8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)**.**

CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	CHAPTER V TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS
Article 40	***Article 40***	***Article 40***	***Article 40***
General principle for transfers	***General principle for transfers***	***General principle for transfers***	***General principle for transfers***
Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.	***deleted***	*Tentative agreement in trilogue:* Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

Article 41	***Article 41***	***Article 41***	***Article 41***
Transfers with an adequacy decision	***Transfers with an adequacy decision***	***Transfers with an adequacy decision***	***Transfers with an adequacy decision***
	Amendment 137		
1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.	1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any ~~further~~***specific*** authorisation.	1. A transfer ***of personal data to a third country or an international organisation*** may take place where the Commission has decided that the third country, or a territory or ***one or more specified*** ~~a processing~~ sector**s** within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any ~~further~~ ***specific*** authorisation.	*Tentative agreement in trilogue:* 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:	2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:	2. When assessing the adequacy of the level of protection, the Commission shall***, in particular, take account of*** ~~give consideration to~~ the following elements:	*Tentative agreement in trilogue:* 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;	(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law ***as well as the implementation of this legislation***, the professional rules and security measures which are complied with in that country or by that international organisation, ***jurisprudential precedents,*** as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;	(a) the rule of law, ***respect for human rights and fundamental freedoms,*** relevant legislation ~~in force~~, both general and sectoral, ***data protection*** ~~including concerning public security, defence, national security and criminal law, the professional~~ rules and security measures***, including rules for onward transfer of personal data to another third country or international organisation,*** which are complied with in that country or ~~by that~~ international organisation, as well as ***the existences of*** effective and enforceable ***data subject*** rights ~~including~~ ***and*** effective administrative and judicial redress for data subjects~~, in particular for those data subjects residing in the Union~~ whose personal data are being transferred;	*Presidency suggestion:* (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, as well as the implementation of this legislation, data protection rules-including concerning public security, defence, national security and criminal law, professional rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, jurisprudential precedents, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and	(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, ***including sufficient sanctioning powers***, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and	(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or ***to which an*** international organisation ~~in question~~ ***is subject, with*** responsib~~le~~***eility*** for ensuring ***and enforcing*** compliance with the data protection rules ***including adequate sanctioning powers*** for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States;~~and~~	*Tentative agreement in trilogue:* (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate sanctioning powers for assisting and advising the data subjects in exercising their rights and for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation in question has entered into.	(c) the international commitments the third country or international organisation in question has entered into***, in particular any legally binding conventions or instruments with respect to the protection of personal data***.	(c) the international commitments the third country or international organisation ~~in question~~ ***concerned*** has entered into ***or other obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data***.	*Tentative agreement in trilogue:* (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.
		2a. The European Data Protection Board shall give the Commission an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.	*Tentative agreement in trilogue:* *Replace the text in Article 66(1)(ce) by:* (ce) give the Commission an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation,

			including correspondence with the government of the third country, territory or processing sector within that third country or the international organisation.
3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	3. The Commission ~~may~~ ***shall be empowered to adopt delegated acts in accordance with Article 86 to*** decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. ~~Those implementing acts~~ ***Such delegated acts*** shall ~~be adopted in accordance with the examination procedure referred to in Article 87(2)~~ ***provide for a sunset clause if they concern a processing sector and shall be revoked according to paragraph 5 as soon as an adequate level of protection according to this Regulation is no longer ensured.***	3. The Commission, ***after assessing the adequacy of the level of protection,*** may decide that a third country, or a territory or ***one or more specified*** ~~a processing~~ sector**s** within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Th~~o~~se implementing act~~s~~ ***shall specify its territorial and sectoral application and, where applicable, identify the (independent) supervisory authority(ies) mentioned in point(b) of paragraph 2. The implementing act*** shall be adopted in accordance with the examination procedure referred to in Article 87(2).	*Tentative agreement in trilogue:* 3. The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities mentioned in point(b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2).

		3a.* Decisions adopted by the Commission on the basis of Article 25(6~~) or Article 26(4)~~ of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission *Decision adopted in accordance with paragraph 3 or 5.	*Tentative agreement in trilogue:* *Move to Article 41(8)*
4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.	4. The ~~implementing~~***delegated*** act shall specify its ~~geographical~~***territorial*** and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.	***deleted***	
	4a. The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the elements listed in paragraph 2 where a delegated act pursuant to paragraph 3 has been adopted.	***4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC.***	*Tentative agreement in trilogue:* 4a. The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).	5. The Commission ~~may~~***shall be empowered to adopt delegated acts in accordance with Article 86 to*** decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure ***or no longer ensures*** an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).~~	5. The Commission may decide that a third country, or a territory or a ~~processing~~ ***specified*** sector within that third country, or an international organisation ~~does not~~ ***no longer*** ensure***s*** an adequate level of protection within the meaning of paragraph 2 ***and may, where necessary, repeal, amend or suspend such decision without retro-active effect*** ~~of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those~~ **The** implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency ~~for individuals with respect to their right to personal data protection~~, in accordance with the procedure referred to in Article 87(3).	*Tentative agreement in trilogue:* 5. The Commission may, in particular following the review referred to in paragraph 3, decide that a third country, or a territory or a specified sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 without retro-active effect. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 87(3).

		5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.	*Tentative agreement in trilogue:* 5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.	6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the ~~Decision~~ ***decision*** made pursuant to paragraph 5 of this Article.	6. ~~Where the Commission decides~~***A decision*** pursuant to paragraph 5~~, any~~ ***is without prejudice to*** transfer***s*** of personal data to the third country, or ~~a~~***the*** territory or ~~a processing~~ ***specified*** sector within that third country, or the international organisation in question ~~shall be prohibited, without prejudice~~ ***pursuant*** to Articles 42 to 44. ~~At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.~~	*Tentative agreement in trilogue:* 6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or specified sector within that third country, or the international organisation in question pursuant to Articles 42 to 44.
	6a. Prior to adopting a delegated act pursuant to paragraphs 3 and 5, the Commission shall request the European Data Protection Board to provide an opinion on the adequacy of the level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation, including correspondence with the government of the third country,		*Tentative agreement in trilogue:* *see 2a*

	territory or processing sector within that third country or the international organisation.		
7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.	7. The Commission shall publish in the *Official Journal of the European Union* ***and on its website*** a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.	7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and ~~processing~~ ***specified*** sectors within a third country and international organisations ~~where it has decided that an adequate level of protection is or is not ensured~~ ***in respect of which decisions have been taken pursuant to paragraphs 3, 3a and 5***.	*Tentative agreement in trilogue:* 7. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of those third countries, territories and specified sectors within a third country and international organisations where it has decided that an adequate level of protection is or is no longer ensured.
8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.	8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until ***five years after the entry into force of this Regulation unless*** amended, replaced or repealed by the Commission ***before the end of this period.***	***deleted***	*Tentative agreement in trilogue:* 3a. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5.

Article 42	***Article 42***	***Article 42***	***Article 42***
Transfers by way of appropriate safeguards	***Transfers by way of appropriate safeguards***	***Transfers by way of appropriate safeguards***	***Transfers by way of appropriate safeguards***
	Amendment 138		
1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.	1. Where the Commission has taken no decision pursuant to Article 41, ***or decides that a third country, or a territory or processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5),*** a controller or processor may ***not*** transfer personal data to a third country, territory or an international organisation ***unless*** the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.	1. ~~Where the Commission has taken no~~ ***In the absence of a*** decision pursuant to ***paragraph 3 of*** Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards~~with respect to the protection of personal data in a legally binding instrument~~***, also covering onward transfers***.	*Presidency suggestion:* 1. In the absence of a decision pursuant to paragraph 3 of Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:	2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:	2. The appropriate safeguards referred to in paragraph 1 ~~shall~~ ***may*** be provided for, ~~in particular~~***without requiring any specific authorisation from a supervisory authority***, by:	*Tentative agreement in trilogue:* 2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
		(oa) a legally binding and enforceable instrument between public authorities or bodies; or	*Tentative agreement in trilogue:* (oa) a legally binding and enforceable instrument between public authorities or bodies; or
(a) binding corporate rules in accordance with Article 43; or	(a) binding corporate rules in accordance with Article 43; or	(a) binding corporate rules ~~in accordance with~~ ***referred to in*** Article 43; or	*Tentative agreement in trilogue:* (a) binding corporate rules in accordance with Article 43; or
	(aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39; or		*see (e)*
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or	***deleted***	(b) standard data protection clauses adopted by the Commission~~Those implementing acts shall be adopted~~ in accordance with the examination procedure referred to in Article 87(2); or	*Tentative agreement in trilogue:* (b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or	(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or	(c) standard data protection clauses adopted by a supervisory authority ~~in accordance with the consistency mechanism referred to in Article 57 when declared generally valid~~ ***and adopted*** by the Commission pursuant to ~~point (b) of Article 62(1)~~***the examination procedure referred to in Article 87(2)***; or	*Tentative agreement in trilogue:* (c) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 87(2); or
(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.	(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.	(d) ***an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or***	*Presidency suggestion:* (d) an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
		(e) an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor (…) in the third country to apply the appropriate safeguards, including as regards data subjects' rights.	*Presidency suggestion:* (e) an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

		2a. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: ***(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the data in the third country or international organisation; or*** ***(b) provisions to be inserted into administrative arrangements between public authorities or bodies.***	*Tentative agreement in trilogue:* 2a. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.	3. A transfer based on standard data protection clauses***, a "European Data Protection Seal"*** or binding corporate rules as referred to in point (a), ~~(b)~~ ***(aa)*** or (c) of paragraph 2 shall not require any ~~further~~***specific*** authorisation.	***deleted***	

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

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

		5a. The supervisory authority shall apply the consistency mechanism in the cases referred to in points (ca), (d), (e) and (f) of Article 57 (2).	*Tentative agreement in trilogue:* 5a. The supervisory authority shall apply the consistency mechanism referred to in Article 57 in the cases referred to in paragraph 2a.
		5b.* Authorisations by *a Member State or* supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission *Decision adopted in accordance with paragraph 2.	*Tentative agreement in trilogue:* 5b. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2.

Article 43	*Article 43*	*Article 43*	*Article 43*
Transfers by way of binding corporate rules	***Transfers by way of binding corporate rules***	***~~Transfers by way of b~~Binding corporate rules***	***Transfers by way of binding corporate rules***
	Amendment 139		
1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:	1. ~~A~~***The*** supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:	1. ~~A~~ ***The competent*** supervisory authority shall **approve binding corporate rules** in accordance with the consistency mechanism set out in Article ~~58~~***57*** ~~approve binding corporate rules~~, provided that they:	*Tentative agreement in trilogue:* 1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 57, provided that they:
(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;	(a) are legally binding and apply to and are enforced by every member within the controller's group of undertakings ***and those external subcontractors that are covered by the scope of the binding corporate rules***, and include their employees;	(a) are legally binding and apply to and are enforced by every member ***concerned of the*** ~~within the controller's or processor's~~ group of undertakings ***or group of enterprises engaged in a joint economic activity***~~, and include their employees~~;	*Tentative agreement in trilogue:* (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings or groups of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects;	(b) expressly confer enforceable rights on data subjects;	(b) expressly confer enforceable rights on data subjects ***with regard to the processing of their personal data***;	*Tentative agreement in trilogue:* (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;
(c) fulfil the requirements laid down in paragraph 2.	(c) fulfil the requirements laid down in paragraph 2	(c) fulfil the requirements laid down in paragraph 2.	*Tentative agreement in trilogue* (c) fulfil the requirements laid down in paragraph 2.
	1a. With regard to employment data, the representatives of the employees shall be informed about and, in accordance with Union or Member State law and practice, be involved in the drawing-up of binding corporate rules pursuant to Article 43.		
2. The binding corporate rules shall at least specify:	2. The binding corporate rules shall at least specify.	2. The binding corporate rules ***referred to in paragraph 1*** shall ~~at least~~ specify **at least** :	*Tentative agreement in trilogue:* 2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings and its members;	(a) the structure and contact details of the group of undertakings and its members ***and those external subcontractors that are covered by the scope of the binding corporate rules***;	(a) the structure and contact details of the ***concerned*** group ~~of undertakings~~ and ***of each of*** its members;	*Tentative agreement in trilogue:* (a) the structure and contact details of the concerned group and of each of its members;
(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	(b) the data transfers or ~~set~~ ***categories*** of transfers, including the ~~categories~~ ***types*** of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	*Tentative agreement in trilogue:* (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
(c) their legally binding nature, both internally and externally;	(c) their legally binding nature, both internally and externally;	(c) their legally binding nature, both internally and externally;	*Tentative agreement in trilogue* (c) their legally binding nature, both internally and externally;

(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;	(d) the general data protection principles, in particular purpose limitation, ***data minimisation, limited retention periods,*** data quality, ***data protection by design and by default,*** legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;	(d) ***application of*** the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of ~~sensitive~~ ***special categories of*** personal data~~;~~**,** measures to ensure data security;**,** and the requirements ~~for~~ ***in respect of*** onward transfers to ~~organisations~~ ***bodies*** ~~which are~~ not bound by the ~~policies~~***binding corporate rules***;	*Tentative agreement in trilogue: subject to redrafting:* (d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	(e) the rights of data subjects ***in regard to the processing of their personal data*** and the means to exercise these rights, including the right not to be subject to ~~a measure based on~~ ***decisions based solely on automated processing, including*** profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	*Tentative agreement in trilogue: subject to alignment with agreement on Article 20:* (e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;	(f) the acceptance by the controller ~~or processor~~ established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller ~~or the processor~~ may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;	(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member ***concerned*** ~~of the group of undertakings~~not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, ~~if he proves~~ ***on proving*** that that member is not responsible for the event giving rise to the damage;	*Tentative agreement in trilogue:* (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage;
(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;	(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;	(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article**s** ~~11~~**14 and 14a**;	*Tentative agreement in trilogue: subject to alignment with agreement on Article 14 and 14a:* (g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 14 and 14a;

(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;	(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;	(h) the tasks of ~~the~~ ***any*** data protection officer designated in accordance with Article 35 ***or any other person or entity in charge of the*** ~~, including~~ monitoring ~~within the group of undertakings the~~ compliance with the binding corporate rules ***within the group***, as well as monitoring the training and complaint handling;	*Tentative agreement in trilogue:* (h) the tasks of any data protection officer designated in accordance with Article 35 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;
		(hh) the complaint procedures;	*Tentative agreement in trilogue:* (hh) the complaint procedures;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;	(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;	(i) the mechanisms within the group ~~of undertakings aiming at~~ ***for*** ensuring the verification of compliance with the binding corporate rules***. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point (h) and to the board of the controlling undertaking or of the group of enterprises, and should be available upon request to the competent supervisory authority***;	*Tentative agreement in trilogue:* (i) the mechanisms within the group for ensuring the verification of compliance with the binding corporate rules**.** Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point (h) and to the board of the controlling undertaking or of the group of enterprises, and should be available upon request to the competent supervisory authority;
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;	(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;	(j) the mechanisms for reporting and recording changes to the ~~policies~~ ***rules*** and reporting these changes to the supervisory authority;	*Tentative agreement in trilogue:* (j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group ~~of undertakings~~, in particular by making available to the supervisory authority the results of ~~the~~ verifications of the measures referred to in point (i) of this paragraph***;***	*Tentative agreement in trilogue:* (k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (i) of this paragraph;
		(l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and	*Tentative agreement in trilogue:* (l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

		(m) the appropriate data protection training to personnel having permanent or regular access to personal data.	*Tentative agreement in trilogue:* (m) the appropriate data protection training to personnel having permanent or regular access to personal data.
		2a. The European Data Protection Board shall advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules	*Move to Article 66*

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the ***format, procedures,*** criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, ***including transparency for data subjects,*** the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	***deleted***	
4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	***deleted***	4. The Commission may specify the format and procedures for the exchange of information ~~by electronic means~~ between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	*Tentative agreement in trilogue:* 4. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

	Amendment 140		
	Article 43a (new)		***Article 43a (new)***
	Transfers or disclosures not authorised by Union law		***Transfers or disclosures not authorised by Union law***
	1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognised or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.		*Tentative agreement in trilogue:* 1. Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

	2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority.		

	3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with points (d) and (e) of Article 44(1) and Article 44(5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57.		
	4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1).		

Article 44	***Article 44***	***Article 44***	***Article 44***
Derogations	***Derogations***	***Derogations for specific situations***	***Derogations for specific situations***
	Amendment 141		
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:	1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:	1. In the absence of an adequacy decision pursuant to ***paragraph 3 of*** Article 41**,** or of appropriate safeguards pursuant to Article 42, ***including binding corporate rules*** a transfer or a ~~set~~ ***category*** of transfers of personal data to a third country or an international organisation may take place only on condition that:	*Tentative agreement in trilogue:* 1. In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or	(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or	(a) the data subject has ***explicitly*** consented to the proposed transfer, after having been informed ~~of the risks of~~ ***that*** such transfers ***may involve risks for the data subject*** due to the absence of an adequacy decision and appropriate safeguards; or	*Presidency suggestion:* (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or	(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or	(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or	*Tentative agreement in trilogue* (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or	(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or	(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or	*Tentative agreement in trilogue* (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important grounds of public interest; or	(d) the transfer is necessary for important grounds of public interest; or	(d) the transfer is necessary for important ~~grounds~~ ***reasons*** of public interest; or	*Tentative agreement in trilogue:* (d) the transfer is necessary for important reasons of public interest; or
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	*Tentative agreement in trilogue* (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or
(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of ~~an~~other person**s**, where the data subject is physically or legally incapable of giving consent; or	*Tentative agreement in trilogue:* (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or	(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case**.**	(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate ***a*** legitimate interest ***but only*** to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or	*Tentative agreement in trilogue:* (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or
(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.	***deleted***	(h) the transfer***, which is not large scale or frequent,*** is necessary for the purposes of the legitimate interests pursued by the controller ***which are not overridden by the interests or rights and freedoms of the data subject*** ~~or the processor, which cannot be qualified as frequent or massive,~~ and where the controller ~~or processor~~ has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced ~~appropriate~~ ***suitable*** safeguards	*Tentative agreement in trilogue:* (h) Where a transfer could not be based on a provision in Articles 41 or 42, including binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which

		with respect to the protection of personal data~~, where necessary~~.	are not overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall in addition to the information referred to in Article 14 and Article 14a, inform the data subject about the transfer and on the compelling legitimate interests pursued by the controller.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	*Tentative agreement in trilogue:* 2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall 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 appropriate safeguards with respect to the protection of personal data, where necessary.	***deleted***	***deleted***	

4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.	4. Points (b)~~,~~ ***and*** (c) ~~and (h)~~ of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.	4. Points ***(a),*** (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.	*Tentative agreement in trilogue:* 4. Points (a), (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.
5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.	5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.	5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the ***national*** law of the Member State to which the controller is subject.	*Tentative agreement in trilogue:* 5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.
		5a. 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 personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.	*Tentative agreement in trilogue:* 5a. 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 personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.	***Deleted***	6. The controller or processor shall document the assessment as well as the ~~appropriate~~ ***suitable*** safeguards ~~adduced~~ referred to in point (h) of paragraph 1 ~~of this Article~~ in the ~~documentation~~ ***records*** referred to in Article 28~~and shall inform the supervisory authority of the transfer~~.	*Presidency suggestion:* 6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in point (h) of paragraph 1 in the records referred to in Article 28.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.	7. The ~~Commission~~ ***European Data Protection Board*** shall be ~~empowered to adopt delegated acts in accordance with Article 86~~ ***entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)*** for the purpose of further specifying ~~'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as~~ the criteria and requirements for ~~appropriate safeguards referred to in point (h)~~ ***data transfers on the basis*** of paragraph 1.	***deleted***	*Move to Article 66*

Article 45	*Article 45*	*Article 45*	*Article 45*
International co-operation for the protection of personal data	***International co-operation for the protection of personal data***	***International co-operation for the protection of personal data***	***International co-operation for the protection of personal data***
	Amendment 142		
1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:	1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:	1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:	*Tentative agreement in trilogue:* 1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;	(a) develop effective international co-operation mechanisms to ~~facilitate~~ ***ensure*** the enforcement of legislation for the protection of personal data;	(a) develop ~~effective~~ international co-operation mechanisms to facilitate the ***effective*** enforcement of legislation for the protection of personal data;	*Tentative agreement in trilogue:* (a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through ~~notification,~~ complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;	*Tentative agreement in trilogue:* (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;	(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;	(c) engage relevant stakeholders in discussion and activities aimed at ~~furthering~~ ***promoting*** international co-operation in the enforcement of legislation for the protection of personal data;	*Tentative agreement in trilogue:* (c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice.	(d) promote the exchange and documentation of personal data protection legislation and practice***;***	(d) promote the exchange and documentation of personal data protection legislation and practice.	*Tentative agreement in trilogue:* (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.
	Amendment 143		
	(da) clarify and consult on jurisdictional conflicts with third countries.		*see (d)*
2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).	2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).	***deleted***	

	Amendment 144		
	Article 45a (new)		***Article 45a (new)***
	Report by the Commission		***Report by the Commission***
	The Commission shall submit to the European Parliament and the Council at regular intervals, starting not later than four years after the date referred to in Article 91(1), a report on the application of Articles 40 to 45. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall be supplied without undue delay. The report shall be made public.		*Tentative agreement in trilogue:* *Incorporate the content of Article 45a new in paragraph 2 and paragraph 2a (new) of Article 90* 1. The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. 2. In the context of these evaluations and reviews, the Commission shall examine, in particular, the application and functioning of the provisions of: (a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 41, paragraph 3 and decisions adopted on the basis of Article 25, paragraph 6 of Directive

			95/46/EC; (b) Chapter VII on Co-operation and Consistency. 2a. For the purpose referred to in paragraphs 1 and 2, the Commission may request information from Member States and supervisory authorities. 2b. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the views and findings of the European Parliament, the Council as well as other relevant bodies or sources.

			Tentative agreement in trilogue: 3. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The reports shall be made public. *Tentative agreement in trilogue:* 4. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society.