Council of the European Union

Brussels, 23 October 2015
(OR. en)

12838/15

Interinstitutional File:
2012/0010 (COD)

LIMITE

DATAPROTECT 159
JAI 731
DAPIX 167
FREMP 208
COMIX 474
CODEC 1315

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	12493/15 12951/15
No. Cion doc.:	5833/12
Subject:	Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data – Preparation of the trilogue – Chapter V

I. INTRODUCTION

1. On 9 October 2015, the Council agreed on a general approach[1] on the proposal for a Directive on the protection of individuals with regards to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (hereafter referred to as the draft Directive), thereby giving the Presidency a negotiating mandate to enter into trilogues with the European Parliament.

[1] 12555/15

2. The Presidency recalls the objective of reaching a conclusion on the whole data protection reform by the end of 2015 in accordance with the conclusions of the European Council of 25-26 June 2015.

3. The first trilogue is scheduled for 27 October 2015[2] and the second one for 9 November 2015.

4. The second trilogue will focus on Chapter V of the draft Directive. With a view to preparing the next trilogue, the Presidency invites delegations to discuss:

    - Article 3(16) - international organisation;

    - Chapter V;

    - Relevant recitals 45 - 50.

II. PREPARATION OF THE SECOND TRILOGUE

5. Considering the position of the European Parliament and the Council's general approach, delegations will note that there is **consensus** on:

    - Article 36(1) (a) and (b) (Council text) and Article 36(2) (a) and (b) (in the EP text);
    - Article 36 (1) (d) subject to the discussions on the scope;

6. The Presidency suggests to maintain the Council's **general approach** as regards:

    - Article 3(16) (definition identical to the one as tentatively agreed in the context of the draft Regulation, except as regards the reference to 'Interpol');

    - Article 33(1) (a);

    - Article 33 (1) (c) reflects the same idea as EP Article 33 (aa);

    - Article 33 (ab) of EP text - suggest to delete;

[2] 12951/15

- Article 33 (b) of the EP text - suggest to delete;
- Article 33(1) (d);
- Article 33(1)(e) reflects the same idea as EP Article 33 (bb) and (bc);
- Article 33 - second part (a) and (b) of the EP text - to reject;
- Article 33(2);
- Article 33(3);
- Article 35;
- Article 36(1)(c), keep 'necessary' rather than 'essential';
- Article 36(1) (e);
- Article 36(2a) of the EP text - to reject; substance should be covered by Article 33 (1) chapeau as amended;
- Article 36(2b) of the EP text- to reject; substance should be covered by Article 33 (1) chapeau as amended;

7. The Presidency considers that in the following Articles the **consistency** with the text of the draft Regulation is necessary and therefore the Articles should be aligned with the compromise text found in the draft Regulation and as set out in document 11246/15 (to which the page references below apply). Delegations are asked to confirm this understanding.

    - Article 33(1) chapeau; align wording, taking into account the tentative agreement in the Regulation (Article 40) (p 44-45) except for the reference to controller and processor;

- Article 34(1) and (2) chapeau - align wording taking into account the tentative agreement in the Regulation (Article 41(1) and (2), p. 46-47), keep general approach as regards using adequacy decisions taken under the Regulation and therefore reject EP proposal that adequacy decision taken by the Commission under the Regulation could not be used for transfers under the Directive.
- Article 34(2)(a), tentative agreement in the Regulation (Article 41(2) (a) p.47), but maintaining the reference to public security, defence, national security and criminal law;
- Article 34(2)(b) and (c), tentative agreement in the Regulation (Article 41(2) (b) and (c) p.47);
- Article 34(2a), tentative agreement in the Regulation (Article 41(2a), p. 49) and therefore move it to Article 49 of the Directive;
- Article 34(3), tentative agreement in the Regulation (Article 41(3), p. 50);
- Article 34(4) of EP text, tentative agreement in the Regulation (Article 41(4), p. 51), this paragraph should be deleted;
- Article 34(4a), tentative agreement in the Regulation (Article 41 (4a), p.51), but as regards the Directive no reference to Directive 95/46
- Article 34 (5), (5a), (6), (7), tentative agreement in the Regulation (Article 41 (5), (5a), (6), (7), p.52-55)
- Article 36 (1) chapeau corresponds to Article 36(2) chapeau of EP text, tentative agreement in the Regulation (Article 42(1), p. 80), excluding the reference to binding corporate rules;
- Article 38 - tentative agreement in the Regulation (Article 45, page 89-91)

- Article 38a - as suggested by EP - tentative agreement in the Regulation (Article 45a, page 92- 94) which means moving the parts that are relevant to the Directive into Article 61 on evaluation.

8. The Presidency takes the view that no additional discussion is necessary on the provisions in points 5-7.

9. With regard to the following provisions the Presidency suggests modifications with a view to **compromise suggestions** to take into account the European Parliament's position.

   - Article 33 (ba) of EP text - with additional flexibility;
   - Article 34(8) of EP text, suggest to go back to COM proposal and to reinsert (8);
   - Article 35(2) of EP text, suggesting to add authorisation by supervisory authority as an alternative condition in Article 35 (1) (c) to guarantee appropriate safeguards;
   - Article 36(2) - delegations are asked for flexibility in light of paragraph 1 of the EP text which reflects a similar idea;
   - Article 36(2c) of the EP text- delegations are asked for flexibility at least as regards documentation;
   - Article 36aa- delegations are asked to consider moving the content to Article 33, while keeping the substance of Article 36aa given that the substance of Article 36aa is a derogation to Article 33(1)(c).
   - Article 37 of the EP text - delegations are asked to be flexible to reinsert Article 37 with the additions made by the EP.

10. The Presidency invites delegations to comment on any other issues pertaining to the provisions in the Annex which they deem important with a view to the trilogue on 9 November 2015.

COM (2012)0010 document 5833/12	EP amendments 2012/0010(COD)	Council general approach document 12555/14	Comments/compromise suggestions
	Amendment 37		
(45) Member States should ensure that a transfer to a third country only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced.	(45) Member States should ensure that a transfer to a third country only takes place if ~~it~~***that specific transfer*** is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the controller in the third country or international organisation is ~~an~~ ***a public*** authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate	(45) Member States should ensure that a transfer to a third country or to an international organisation only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced or when derogations for specific situations apply.	

	safeguards have been adduced***, or where appropriate safeguards have been adduced by way of a legally binding instrument***. ***Data transferred to competent public authorities in third countries should not be further processed for purposes other than the one they were transferred for***.		
	Amendment 38		
	(45a) Further onward transfers from competent authorities in third countries or international organisations to which personal data have been transferred should only be allowed if the onward transfer is necessary for the same specific purpose as the original transfer and the second recipient is also a competent public authority. Further onward transfers should not be allowed for general law-enforcement purposes. The competent authority that carried out the original transfer should have agreed to the onward transfer.	(45a) Where personal data are transferred from a Member State to third countries or international organisations, such transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Members State is so immediate as to render it impossible to obtain prior authorisation in good time,	

		the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries and/or international organisations.	
(46) 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.	(46) 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.	(46) Where the Commission has not adopted a decision in accordance with Article 41 of Regulation (EU) XXX, it may decide with effect for the entire Union that certain third countries, or a territory or one or more specified 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 (…) specific authorisation.	

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how the rule of law, access to justice, as well as international human rights norms and standards, in that third country are respected.	(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how the rule of law, access to justice, as well as international human rights norms and standards, in that third country are respected.	(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should 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 (…).	
	Amendment 39		
(48) The Commission should equally be able to recognise that a third country, or a territory or a processing sector within a third country, or an international organisation, does not offer an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third	(48) The Commission should equally be able to recognise that a third country, or a territory or a processing sector within a third country, or an international organisation, does not offer an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third	(48) The Commission should equally be able to 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 35-36 are fulfilled. Provision should be made for procedures for consultations between the Commission and such third	

countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards or on the basis of a derogation laid down in the Directive.	countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards ***by means of legally binding instruments*** or on the basis of a derogation laid down in this Directive.	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 40		
(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or 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, considers that appropriate safeguards with respect to the protection of personal data exist. In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of	(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data ~~or 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, considers that appropriate safeguards with respect to the protection of personal data exist. In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the~~	(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or where the controller (…) has assessed all the circumstances surrounding the data transfer (…) and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. Such legally binding instruments could for example be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and may be enforced by their data subjects, ensuring compliance with data	

the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims.	~~data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims~~.	protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress**.** The controller may take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller may also take into account that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition the controller should take into account that the personal data will not be used to request, hand down or execute the death penalty or any form of cruel and inhuman treatment. While these conditions could be considered as appropriate safeguards allowing the transfer of data, the controller may require additional safeguards.	

	Amendment 41		
	(49a) In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims. ***Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfer of personal data and should not allow wholesale transfer of data which should be limited to data strictly necessary. Moreover, the decision***	(49aa) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could only take place in specific situations if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is necessary for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or necessary in an individual case for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of public security, or necessary in an individual case for the establishment, exercise or defence of legal claims**.**	

	for transfer should be made by a duly authorised person and that transfer must be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.		
		(49b) Competent authorities of Member States are applying bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial co-operation in criminal matters and police co-operation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through or at least with the cooperation of the competent authorities of the concerned third countries. However, in specific individual cases, it may occur that the procedures provided for by the international agreements applicable do not allow to exchange the relevant information in a timely manner, so that competent authorities of Member States have to transfer personal data directly to recipients established in third	

		countries. This may be the case when criminal offences have been committed by means of electronic communication technology like social networks, or where data generated by communication technology are relevant as evidence of the perpetration of a criminal offence or where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence. Even if this exchange between competent authorities and recipients established in third countries should only take place in individual and specific cases, this Directive should provide for conditions to regulate such cases. These provisions should not be considered as derogations to any existing bilateral or multilateral international agreements in the field of judicial co-operation in criminal matters and police co-operation. These rules should apply in addition to the other rules of the Directive, in particular those on the lawfulness of processing and of Chapter V.	

(50) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. 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. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.	(50) When personal data move across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. 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. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.	(50) deleted	

Article 3	***Article 3***	***Article 3***	
Definitions	***Definitions***	***Definitions***	
	Amendment 61		
		(16) '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 as well as Interpol.	

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 33	***Article 33***	***Article 33***	
General principles for transfers of personal data	***General principles for transfers of personal data***	***General principles for transfers of personal data***	
	Amendment 96		
Member States shall provide that any transfer of personal data by competent authorities that is undergoing processing or is intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:	Member States shall provide that any transfer of personal data by competent authorities that are undergoing processing or are intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:	1. Member States shall provide that any transfer of personal data by competent authorities (…) to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:	

(a) the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and	(a) the ***specific*** transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and	(a) the transfer is necessary for the purposes set out in Article 1 (1); and,	
	(aa) the data are transferred to a controller in a third country or international organisation that is a public authority competent for the purposes referred to in Article 1(1); and	(c) the controller in the third country or international organisation is an authority competent for the purposes set out in Article 1(1); and	
	(ab) the conditions laid down in this Chapter are complied with by the controller and the processor, including for onward transfers of personal data from a third country or an international organisation to another third country or to another international organisation; and		
(b) the conditions laid down in this Chapter are complied with by the controller and processor.	(b) the ~~conditions laid down in this Chapter~~ ***other provisions adopted pursuant to this Directive*** are complied with by the controller and processor~~.~~***; and***	***Deleted***	

	(ba) the level of protection of the personal data individuals guaranteed in the Union by this Directive is not undermined; and		
	(bb) the Commission has decided under the conditions and procedure referred to in Article 34 that the third country or international organisation in question ensures an adequate level of protection; or	(d) in case personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in compliance with its national law and	
	(bc) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument as referred to in Article 35.	(e) the Commission has decided pursuant to Article 34 that the third country or international organisation in question ensures an adequate level of protection or in the absence of an adequacy decision pursuant to Article 34, where appropriate safeguards are adduced or exist pursuant to Article 35.	
	Member States shall provide that further onward transfers referred to in paragraph 1 of this Article may only take place if, in addition to the conditions laid down in that paragraph:	2. Member States shall provide that transfers without the prior authorisation by another Member State in accordance with point (d) shall be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to	

		public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.	
		3. Member States shall provide that in the absence of an adequacy decision pursuant to Article 34 or of appropriate safeguards in accordance with Article 35, a transfer may only take place where derogations for specific situations apply pursuant to Article 36 and the conditions laid down in points (a), (c) and (d) of paragraph 1 and, as the case may be, (…) in paragraph 2 of this Article are complied with.	
	(a) the onward transfer is necessary for the same specific purpose as the original transfer; and		
	(b) the competent authority that carried out the original transfer authorises the onward transfer.		

Article 34	***Article 34***	***Article 34***	
Transfers with an adequacy decision	***Transfers with an adequacy decision***	***Transfers with an adequacy decision***	
	Amendment 97		
1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) …./2012 or in accordance with paragraph 3 of this Article 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. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided ~~in accordance with Article 41 of Regulation (EU) …./2012 or~~ in accordance with paragraph 3 of this Article 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. Member States shall provide that a transfer of personal data to a third country or a territory or one or more specified sectors within a third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation EU/XXX or in accordance with paragraph 3 of this Article that the third country or a territory or specified sector 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. Where no decision adopted in accordance with Article 41 of Regulation (EU) …./2012 exists, the Commission shall assess the adequacy of the level of protection, giving consideration to the following elements:	2. ~~Where no decision adopted in accordance with Article 41 of Regulation (EU) …./2012 exists~~***When assessing the adequacy of the level of protection***, the Commission shall ~~assess the adequacy of the level of protection, giving~~ ***give*** consideration to the following elements:	2. Where no decision adopted in accordance with Article 41 of Regulation EU/XXX (…) applies, the Commission shall assess the adequacy of the level of protection, in particular taking into account 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 as well as the 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 and the*** 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, both general and sectoral, data protection rules (…)including concerning public security, defence, national security and criminal law as well as (…) 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 existence of effective and enforceable data subject rights and effective administrative and judicial redress for 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 subject 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 subject in exercising his or her 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 is subject, with responsibility (…) for ensuring and enforcing compliance with the data protection rules including adequate sanctioning powers for assisting and advising (…) data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of 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 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.	

		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.	
3. The Commission may decide, within the scope of this Directive, 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 57(2).	3. The Commission ~~may~~ ***shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 56 to*** decide, within the scope of this Directive, 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 57(2).~~	3. The Commission after assessing the adequacy of the level of protection, may decide, within the scope of this Directive 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 specify its territorial and sectoral application and, where applicable, identify the 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 57(2).	

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 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 that could affect the fulfilment of the elements listed in paragraph 2 in third countries and international organisations in relation to which a delegated act pursuant to paragraph 3 has been adopted.	4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3.	

5. The Commission may decide within the scope of this Directive 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, 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 whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(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 57(3).	5. The Commission ~~may~~***shall be empowered to adopt delegated acts in accordance with Article 56 to*** decide within the scope of this Directive 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, 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 whose personal data are being transferred. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(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 57(3).~~	5. The Commission may decide within the scope of this Directive 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 may, where necessary, repeal, amend or suspend such decision without retro-active effect. The (…) implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 57(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.	Moved from Article 34(6)
6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, that 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, this decision shall be without prejudice to transfers under Article 35(1) or in accordance with Article 36. 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. Member States shall ensure that where the Commission decides pursuant to paragraph 5, ~~that~~ 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~~, this decision shall be without prejudice to transfers under Article 35(1) or in accordance with Article 36~~. 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. Member States shall ensure that where a decision pursuant to paragraph 5 is taken, such decision (…) shall be without prejudice to transfers of personal data to the third country, or the territory or the specified sector within that third country, or the international organisation in question pursuant to Articles 35 and 36 (…).	

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 or an international organisation 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 sectors within a third country or an international organisation 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 specified sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 (…) and 5.	
8. The Commission shall monitor the application of the implementing acts referred to in paragraphs 3 and 5.	8. The Commission shall monitor the application of the ~~implementing~~ ***delegated*** acts referred to in paragraphs 3 and 5.	***deleted***	

Article 35	***Article 35***	***Article 35***	
Transfers by way of appropriate safeguards	***Transfers by way of appropriate safeguards***	***Transfers by way of appropriate safeguards***	
	Amendment 98		
1. Where the Commission has taken no decision pursuant to Article 34, Member States shall provide that a transfer of personal data to a recipient in a third country or an international organisation may take place where:	1. Where the Commission has taken no decision pursuant to Article 34, ~~Member States shall provide that a~~ ***or decides that a third country, or a territory within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 34(5), a controller or processor may not*** transfer ~~of~~ personal data to ~~a recipient in~~ a third country***, or a territory within that third country,*** or an international organisation ~~may take place where:~~ ***unless the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.***	(…) In the absence of a decision pursuant to paragraph 3 of Article 34, Member States shall provide that (…) a transfer of personal data to a third country or an international organisation may take place where:	

(a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument; or	***deleted***	(a) appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding (…) instrument; or	
(b) the controller or processor has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data.	***deleted***	(b) the controller (…) has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data. Such an assessment may take into account the existing cooperation agreements between Europol and/or Eurojust and third countries which allow for the exchange of personal data.	
2. The decision for transfers under paragraph 1 (b) must be made by duly authorised staff. These transfers must be documented and the documentation must be made available to the supervisory authority on request.	2.~~The decision for transfers under paragraph 1 (b) must be made by duly authorised staff.~~ Those transfers must be ~~documented and the documentation must be made available to the supervisory authority on request~~***authorised by the supervisory authority prior to the transfer***.	***deleted***	

Article 36	*Article 36*	*Article 36*	
Derogations	***Derogations***	***Derogations for specific situations***	
	Amendment 99		
By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:	***1. Where the Commission decides pursuant to Article 34(5) that an adequate level of protection does not exist, personal data may not be transferred to the third country or to the international organisation in question if, in the case in question, the legitimate interests of the data subject in preventing any such transfer outweigh the public interest in transferring such data.***	1. (…) In the absence of an adequacy decision pursuant to Article 34 or appropriate safeguards pursuant to Article 35, Member States shall provide that, a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on condition that:	
	2. By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:		
(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or	(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or	(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or	

(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or	(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or	(b) the transfer is necessary to safeguard legitimate interests of the data subject (…) where the law of the Member State transferring the personal data so provides; or	
(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or	(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or	(c) the transfer of the data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country; or	
(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or	(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or	(d) the transfer is necessary in individual cases for the purposes set out in Article 1 (1); or	
(e) the transfer is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.	(e) the transfer is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.	(e) the transfer is necessary in an individual cases for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1 (1).	

		2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.	
	2a. Processing based on paragraph 2 must have a legal basis in Union law, or the law of the Member State to which the controller is subject; that law must meet public interest objective or the need to protect the rights and freedoms of others, respects the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.		
	2b. All transfers of personal data decided on the basis of derogations shall be duly justified and shall be limited to what is strictly necessary, and frequent massive transfers of data shall not be allowed.		

	2c. The decision for transfers under paragraph 2 must be made by duly authorised staff. Those transfers must be documented and the documentation must be made available to the supervisory authority on request, including the date and time of the transfer, information about the recipient authority, the justification for the transfer and the data transferred.		

Article 36aa	***Article 36aa***	***Article 36aa***	
		Transfer of personal data to recipients established in third countries	
		1. By way of derogation from Article 33 (1) (c) and without prejudice to any international agreement referred to in paragraph 2, Union or Member States law may provide that the competent authorities may, in individual and specific cases, transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and the following conditions are fulfilled:	

		(a) the transfer is strictly necessary for the performance of a task of the competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1); and	
		(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand.	
		2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial co-operation in criminal matters and police co-operation.	

Article 37	***Article 37***	***Article 37***	
Specific conditions for the transfer of personal data	***Specific conditions for the transfer of personal data***	***Specific conditions for the transfer of personal data***	
	Amendment 100		
Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met.	Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met. ***The controller shall also notify the recipient of the personal data of any update, rectification or erasure of data, and the recipient shall in turn make the corresponding notification in the event that the data have subsequently been transferred.***	deleted	

Article 38	***Article 38***	***Article 38***	
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 101		
1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:	1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:	***deleted***	
(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;	***deleted***	
(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;	***deleted***	

(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;	***deleted***	
(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~~.~~***;***	***deleted***	

	Amendment 102		
	(da) clarify and consult on jurisdictional conflicts with third countries.		
2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with 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 34(3).	2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with 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 34(3).	***deleted***	

	Amendment 103		
	Article 38a		
	Report by the Commission		
	The Commission shall submit a report on the application of Articles 33 to 38 to the European Parliament and to the Council at regular intervals. The first report shall be submitted not later than four years after the entry into force of this Directive. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall supply that information without undue delay. The report shall be made public.		