COUNCIL OF THE EUROPEAN UNION

Brussels, 23 April 2014

6723/6/13 REV 6

LIMITE

DATAPROTECT 20
JAI 130
MI 131
DRS 34
DAPIX 30
FREMP 15
COMIX 111
CODEC 394

Interinstitutional File: 2012/0011 (COD)

NOTE

from:	General Secretariat
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	16529/12 DATAPROTECT 133 JAI 820 MI 754 DRS 132 DAPIX 146 FREMP 142 COMIX 655 CODEC 2745 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155
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) - Comments on Chapter V

Further to the invitation by the Presidency (CM 1276/1/13 REV 1) delegations have sent in written comments on Chapter V of the 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.

The comments received at 23 April 2014 are set out hereafter.

TABLE OF CONTENT

BELGIUM

Article 40 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.

BE thinks that if a transfer occurs on the basis of the adequacy of a third country's data protection law, an onward transfer from that country must comply with that country's law, not with the Regulation.

Any other interpretation would make adequacy determinations superfluous (e.g., how would this be compatible with the Safe Harbor "Onward transfer" principle).

BE: What are the consequences of the Article 40 on the existing international agreements?

Article 41 Transfers with an adequacy decision

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.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to 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;

(b) the existence and effective functioning of one or more independent supervisory authorities ***and judicial authority*** *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*

(c) the international commitments the third country or international organisation in question has entered into.

BE: *"...the existence and effective functioning of one or more independent supervisory authorities* ***and judicial authority*** *…»*

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).

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.

BE*: 4. The implementing act shall specify its geographical and sectoral application, and, ~~where applicable,~~ identify ~~the supervisory authority~~* ***independent supervisory authority*** *mentioned in point (b) of paragraph 2.*

~~*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).*~~

~~*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.*~~

~~*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.*~~

BE is not in favour of a black list. Paragraphs 5, 6 and 7 of the Article 41 should be deleted.

Article 42 Transfers by way of appropriate safeguards

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.

2.The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

(a) binding corporate rules in accordance with Article 43; or

(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

(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

(d) contractual clauses between the controller or processor and the recipient of the data, which can be a sub-processor, authorised by a supervisory authority in accordance with paragraph 4.

BE: *(d) contractual clauses between the controller or processor and the recipient of the data, which can be a sub-processor…"*

In the proposed Regulation, standard clauses do not extend to agreements between processors and sub-processors. This gap could significantly disadvantage European firms, including new technology start-ups.

BE also proposes to modify the recital 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 and processors and processors and sub-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. In some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust safeguards via additional contractual commitments that supplement standard data protection clauses***".**

BE thinks that it would be a good idea to adapt the all regulation to take into account the situation with the sub processor.
To that extent, BE proposes:

- A definition of the sub-processor (for Article 4): *'sub-processor' means the processor processing personal data on behalf of another processor or sub-processor*.

- Modifications in Article 26:
1°) Art.26.2 d): *"determine the conditions for enlisting another processor or a sub-processor"*.
2°) NEW Art.26.4: "*Paragraph 2 shall not apply where a processing operation is carried out by a sub-processor and the processing is governed by a contract or other legal act binding the sub-processor to the processor [and stipulating in particular that the sub-processor will be subject to the same obligations as those imposed by the controller on the processor pursuant to paragraph 2, taking into account the role and processing activities performed by the sub-processor.]*

(e) contractual clauses between the controller or processor and the recipient of the data that supplement standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and are authorised by the competent supervisory authority in accordance with paragraph 4.

BE believes that these baseline protections should be viewed as a minimum. In many cases, it may be appropriate for organisations to apply additional safeguards to protect data being transferred out of Europe -- i.e. to supplement the standard clauses with even more robust protections. The amendment creates an incentive to adopt these supplemental protections

f) (new) Cooperation agreements or unilateral undertaking by public authorities

BE wants to add a point "(f) *Cooperation agreements or unilateral undertaking by public authorities*";

BE wants to give a solution for public authority and for already existing agreements.
For BE, the notion of "*administrative arrangements providing the legal basis for such transfer"form the 42.5* is not clear and gives not legal certainty for public authorities.
Moreover, BE wants to be sure to cover, for example, the international health regulations.

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.

4. Where a transfer is based on contractual clauses as referred to in point (d) or (e) 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 competent 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.

BE proposes to add the paragraph (e) to be consistent with the new paragraph proposed in Article 42.2.

5. Where public authorities make use of appropriate safeguards with respect to the protection of personal data ~~are~~ but not provided for in a legally binding instrument provided in §2 lit. f), it ~~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 legal 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.

BE wants to modify the paragraph 5 of the Article 42. The model contracts and BCR do not apply to public authorities. The later should be enable to make use of cooperation agreements or unilateral undertaking at it is the case in practice. The paragraph 5 (MoU solutions) intends to address the situation of the public sector and it should be clearly limited to it.

The reference to Article 34 (1) is not relevant anymore because this §1 of the Article 34 is deleted in the new version of the text of the regulation.

6. 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 mitigate the risks involved for the data subjects where a controller [or processor] adopts contractual clauses as provided for in point (d) of paragraph (2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in paragraph (5) for the transfer of personal data to a third country or an international organisation.

6bis. « *In the event of a discrepancy between the Regulation and the legal requirements of the requesting third country, the Commission will strive to resolve the conflicting legal situation during which the data controller or processor cannot be held liable*.»

BE proposes to add a new paragraph to clarify the risk of conflict of law between the draft regulation and laws of third countries. The aim is to avoid new « Swift case » and PNR case.

Article 43 Transfers by way of binding corporate rules

As a general remark, BE would like to underline the fact that it is important that the BCR already accepted should remain in application.

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, 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 their subprocessors, and include their employees;

BE proposes to complete de point (a) in order to cover the sub-processors. In the cloud, cloud providers often use the external subcontractors to perform a specific task to deliver 24/7 service and maintenance. Therefore, this should be recognised in the BCR by the supervising authority.

(b) expressly confer to data subject the rights listed in Articles [xyz], which are enforceable through effective administrative and judicial redress
~~enforceable rights on data subjects~~;

BE proposes a new wording in order to be more clear.

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify:

(a) the structure and contact details of the group of undertakings and its members and their subprocessors;

BE proposes to complete de point (a) in order to cover the sub-processors. In the cloud, cloud providers often use the external subcontractors to perform a specific task to deliver 24/7 service and maintenance. Therefore, this should be recognised in the BCR by the supervising authority.

(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;

(d) the general data protection principles, in particular purpose limitation, data quality as forseen by Article 5(c) and 5(d), 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;

BE proposes a new wording in order to be more clear.

(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;

(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;

(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;

(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;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;

(j) the existence of a suitable training program;

(k) the existence of a complaint handling process by a clearly identified department or person who has an appropriate level of independence in the exercice of his/her functions;

BE thinks that this point should also contain an internal system for handling the complaints

(l) where a member of the group of undertaking has reasons to believe that its national legislation will prevent the compliance with the Bindin corporate group, the commitment to ensure the transparence inside of the corporate group about his problem, but also toward the competent European supervisory authority;

(m) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;

(n) 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.

Article 44 Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42 or of BCR's pursuant to Article 43, 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:

BE: The Article 43 (BCR's) is not mentioned in paragraph 44.1, which should be added.

(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

BE thinks that this is not consistent with the Article 7.4 of the Regulation. Indeed if Article 7.4 of the proposition of Regulation will not be adapted in a way that consent can provide a legal basis for the processing in the relationship Employer-Employee, than Article 44(1)(a) has to be adapted determinating that consent can provide a legal basis for transfer of personal data to third countries in the relationship employer-employee.

(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

(d) the transfer is necessary for important grounds of public interest; or

(dbis) NEW: the transfer is necessary in the context of a public health ermergency siuation; or

BE wants to cover the case where there is a public health ermergency siuation.

(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

(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

(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.

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.

A transfer of personal data to third country public authorities which is necessary for the data controller or processor to comply with that third country's national laws, including laws aimed at the prevention of money laundering or the fight against terrorist financing, shall be legitimized on the basis of point (h) of paragraph 1.

BE proposes to add a new subparagraph in the point 3 of the Article 44. The Regulation offers a unique opportunity to reconcile both the AML/CFT (Prevention of money laundering/fight against terrorist financing) and data protection interests by expressly legitimizing data transfers to third country public authorities for AML/CTF purposes, possibly subject to strict conditions to be defined (e.g. data minimization and data security).

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.

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.

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.

~~*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.persons or if they are to be the recipients.*~~

Article 45 International co-operation for the protection of personal data

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;

(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;

(d) promote the exchange and documentation of personal data protection legislation and practice.

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).

CZECH REPUBLIC

The comments are made in relation to document 16529/12.

CZ focuses on Articles only, as the recitals would have to be adapted later.

In general

CZ wishes to point out that comments given below are without prejudice to horizontal questions and issues, such as delegated and implementing acts or legal form of the proposal. Given the fact that these horizontal issues are being discussed separately, CZ did not specifically comment e.g. on provisions establishing implementing or delegated powers.

Article 40

Given that the recipient of personal data within the third country is expected to comply with legal framework of that country rather that with conditions laid down in Chapter V, CZ does not see any added value of this Article and proposes it to be deleted.

Since many existing treaties from many different areas of public administration may entail transfer of personal data to third countries, and due to the significant changes made to data protection rules as compared to current Directive, CZ believes that a "grandfather clause" along the lines of Article 26 of Council Framework Decision 2008/977/JHA is necessary.

Article 41

- Paragraph 1 should be amended:

„A transfer may take place where the Commission**, after obtaining consent of the European Data Protection Board,** 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."

CZ believes that EDPB should be formally involved in adequacy decisions by giving its consent. Article 66 should be then amended to provide for such consents to be adopted by the EDPB. Alternatively, CZ would support the involvement of Member States.

- Paragraph 2 should be amended:

"When assessing the adequacy of the level of protection, the Commission **and the European Data Protection Board** shall give consideration to the following elements**, with due regard to provisions of this Regulation**:

(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~~;

(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

(c) the international commitments **on protection of privacy and personal data** the third country or international organisation in question has entered into.

Due regard to provisions of this Regulation should provide corresponding parameters for consideration of third countries' data protection rules and systems.
Public security, national security and defence are not within the EU competence and are excluded pursuant to Article 2(2)(a) of the draft Regulation.
The redress should enable efficient enforcement of rights. The exact type of redress mechanism is not that important (independent specialized administrative body may be even more efficient than court).
The last part of (a) sounds like discrimination of EU citizens residing in third countries.
¨The international commitments should be more specified, as many commitments would not be relevant at all.

- Paragraph 3 should be amended:

„The Commission**, after obtaining consent of the European Data Protection Board,** 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).“

CZ believes that EDPB should be formally involved in adequacy decisions by giving its consent. Article 66 should be then amended to provide for such consents to be adopted by the EDPB. Alternatively, CZ would support the involvement of Member States.

- Paragraph 5 should be amended:

“The Commission**, after obtaining consent of the European Data Protection Board,** may **suspend or revoke a decision** ~~decide~~ that a third country, or a territory or a processing sector within that third country, or an international organisation **ensures** ~~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).”

There is no point in adopting “inadequacy decision”, as any transfer to third country must be based on Articles 41 – 44. There may be added value, however, in enabling the EU to react quickly to unfavourable developments in specific third countries that have already been found to ensure adequate protection in the past.

- Paragraph 6 should be deleted.

There is no added value in this provision, as any transfer to third country must be based on Articles 41 – 44. The strictest time limit in this Article (“at the appropriate time”) may be also sacrificed.

- Paragraph 7 should be amended:

„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 **or where such decision has been suspended**."

Changes resulting from changes to paragraph 5. Revoked decisions would be simply struck out of list of adequacy decisions.

- Paragraph 8 should be amended:

„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**, but no longer than four years from the date referred to in Article 91 paragraph 1**."

CZ wishes to prevent jurisdiction shopping. It is inconceivable that EU businesses compliant with this Regulation would be able to maintain their competitiveness vis-à-vis businesses in jurisdictions that were found to provide adequate protection based on 1995 Directive.

Article 42

- Paragraph 2 should be amended to include new point:

"(e) agreement between Member State and third country or international organization."

It is matter of course that such legally binding agreements must provide for appropriate safeguards with respect to the protection of personal data. Reference to elements given by Article 43(2)(b), (d), (e), (f) and (k) could be included mutatis mutandis.

- Paragraphs 4 and 5 should be amended so that non-functional references to Article 34(1)(a) is deleted, as Article 34 now deals with prior consultation only and authorization is provided for by new paragraph 6 of Article 42.

Article 44

- Paragraph 1(a) should be amended:

"(a) the data subject has consented to the proposed transfer, after having been informed of the **fact that** ~~risks of~~ such transfers **may involve increased risk** due to the absence of an adequacy decision and appropriate safeguards; or"

CZ does not wish to burden e.g. small travel bureaus with obligation to research about risks that transfers in such cases may involve in relation to particular country or location. The data subject should simply be notified, prior to his or her consent, that there is neither adequacy decision nor appropriate safeguards and that such transfers may put personal data at increased risk.

GERMANY

In its communication of 23 January 2013, the Presidency invited Member States to submit, by 22 February 2013, proposals for amendments and comments – other than those already submitted in the Council's DAPIX Working Party – on Articles 40 to 45 of Chapter V of the Commission proposal for a General Data Protection Regulation.

A. Preliminary remark

We would like to thank the Presidency for this opportunity to comment. The proposals set out below should be regarded as provisional, non-exhaustive contributions to further discussion of the legal act. We reserve the right to submit further comments, including on fundamental issues which cut across various articles. Notes on the drafting and comments on the German-language version will be made at a later date. The recitals will be commented on separately. Other comments made by Germany in DAPIX meetings will, as a precautionary measure, also be included in the following which will mean some repitition.

B. General remarks

- We believe **the procedure for decisions on adequacy** is in need of critical review. In particular, it is important to preclude the possibility of "forum shopping" in third countries on which an adequacy decision has been made. If an adequacy decision privileges a third country in the exchange of information and puts it on an equal footing with countries within the EU legal system, we must make sure that the data-protection provisions are implemented and interpreted in a uniform manner in that country, in line with the Regulation's aims for the EU. This could be done, for example, by having the consistency mechanism involve the data-protection supervisory authorities of third countries on which an adequacy decision has been adopted.

- Clearer rules are needed on the **status and role of supervisory and monitoring authorities in third countries** and the possible ways in which they can work together with EU data-protection supervisory authorities. Procedural rules should be developed as part of Articles 44 to 45, governing how supervisory authorities in third countries for which an adequacy decision exists are to participate in the consistency mechanism.

- Furthermore, practical experience with the existing procedure has shown that the necessary checks take a long time and mainly affect smaller countries. If a system of such decisions is kept, adequacy assessments for further countries should be started in a timely manner; additionally, a more transparent and more efficient procedure should be developed (cf. our proposal in relation to Article 41(3)).

- In Articles 40 to 45, the question of what **effects** the overall approach to the transfer of data to third countries **will have on the Internet** remains unanswered (cf. *Lindqvist* decision). Clear coverage is particularly lacking for modern IT configurations such as **cloud computing**. Given the significant role played by such technologies in practice, proposals for solutions need to be put forward. One particular issue requiring clarification is that of how European data-protection standards can be guaranteed for data transferred to a cloud located in a third country.

- Articles 40 to 45 should make a clearer distinction between the obligations of the controller and of the processor – this is of particular importance in relation to cloud computing.

- A **balance** needs to be struck in Chapter V **between adequacy decisions, safeguards and derogations**. Chapter V starts by setting out strict, formalised arrangements (adequacy decision, appropriate safeguards, binding corporate rules), which contrast with the very broadly worded derogations that follow. For example, under point (d) of Article 44(1), a transfer of data is still permissible on important grounds of public interest, and point (h) of Article 44(1) allows a transfer for the purposes of the legitimate interests of the controller, without requiring those interests to outweigh the interests of the data subject. The individual derogations therefore need to be examined in detail.

- Stronger overall emphasis should be placed on the principle of **accountability** in Articles 44 et seq.

- In assessments of adequacy, account should also be taken of whether the country or international organisation in question has signed up to international agreements on data protection (particularly Convention 108) and whether it participates in suitable international data-protection systems (e.g. APEC and ECOWAS) (cf. the suggested additions in points (c) and (d) of Article 41(2)).

- Decisions adopted under Article 25(6) or Article 26(4) of Directive 95/46/EC should be reviewed by the Commission after the Regulation has entered into force (cf. our proposal for Article 41(8)).

- The relationship between the draft Regulation and existing data-protection agreements between Member States and third countries or international organisations remains undefined. Provisions above and beyond the reference in recital (79) should be adopted to clarify the matter.

- An **extended procedure** should be provided **for cases in which, ultimately, an adequacy decision is not adopted**. In past cases in which a country's level of data protection was not deemed to be adequate within the meaning of Directive 95/46/EC, the Commission merely refrained from adopting an adequacy decision (e.g. in the case of Australia). In our view, however, the applicant countries and organisations should also be formally notified as to why it was not possible to reach a positive decision and as to the measures they need to take to achieve adequacy. A dialogue should be entered into soon afterwards (and not just "at the appropriate time", as provided in Article 41(6)). On this issue, please also see the suggested new version of Article 41(5).

- The **provisions on negative adequacy decisions contained in paragraphs (5) and (6) of Article 41 should be deleted in their entirety.** Such decisions would send a negative political signal; besides, they would not add any value in practice, as Articles 42 to 44 are to apply even if a negative adequacy decision has been made (Article 41(6): "without prejudice to Articles 42 to 44").

- We enter a scrutiny reservation on the applicability of Articles 40 to 45 to the public sector.

C. Comments on Articles 40 to 45

We stand by our general scrutiny reservations and reservations on individual provisions, as presented in DAPIX and in comments on Articles 40 to 45.

Article 40 ***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.	*Article 40* ***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 (…) both the conditions laid down in this Chapter and the other provisions of this Regulation are complied with by the controller and the processor. This shall also apply to onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.
Article 41 ***Transfers with an adequacy decision*** 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.	*[Article 41* ***Transfers with an adequacy decision*** 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.

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:
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, <u>including legislation</u> 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;
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 (<u>including adequate powers of sanction</u>), 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

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 its accession to international agreements[1] d) participation in a suitable international data protection system established in third countries or a territory or a processing sector[2], and e) ways of ensuring consistent interpretation and application of the data-protection provisions under Articles 55 et seq. The Commission shall, as early as possible, give the European Data Protection Board and the Member States the opportunity to comment on each adequacy assessment.

[1] Such agreements may include, in particular, the Council of Europe's Convention 108.

[2] We propose that the list of checks in Article 42(2) should include a new component consisting of the participation of third states or international organisations in international data-protection systems (e.g. APEC and ECOWAS). Although those systems are still in the early stages of practical implementation, the draft Regulation should make allowance right away for the significance they may gain in future. Point (d) of Article 41(2) requires the systems to be fundamentally suited to ensuring compliance with data protection standards. We further propose, in point (f) of Article 42(2), allowing international data-protection systems to be "recognised by the Commission pursuant to the examination procedure referred to in Article 87(2)" and to function as appropriate safeguards.

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 shall develop and adopt a binding procedure for the assessment of adequacy, which shall set out, in particular, the formal application requirements and the rights and duties of applicants. As part of that procedure, major stakeholders, particularly representatives of the research and business communities, consumer protection organisations and citizens, shall be given the opportunity to comment. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2). The Commission shall ensure the external transparency of the procedure for assessing adequacy. The Commission may, after the procedure for assessing adequacy has been completed, 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. The implementing act shall be adopted in accordance with the examination procedure set out in Article 87(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 act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.
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. If the Commission finds that there is not an adequate level of protection within the meaning of paragraph 1, it shall inform the third country or international organisation in question of the reasons and propose measures for achieving adequacy. The Commission shall, in a timely manner, enter into discussions with the third country or international organisation in question.

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.	
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* 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 (…) 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[1] shall be reviewed following the entry into force of this Regulation. The Commission shall report to the Council and to the Parliament on the outcome of its review and the steps taken. The European Data Protection Board shall be given an advance opportunity to comment on the report. 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 in accordance with the examination procedure referred to in Article 87(2).

[1] It should be clarified that the Safe Harbour Decision falls under Article 41(8).

Article 42 ***Transfers by way of appropriate safeguards***	*Article 42* ***Transfers by way of appropriate safeguards***
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, 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. 1a. The relevant safeguards shall relate in particular to the fact that: (a) compliance with the principles relating to personal data processing pursuant to Article 5 is ensured; (b) the data subject's rights pursuant to Chapter III are protected and effective legal remedies are available; (c) the principles of data protection by design and by default pursuant to Article 23 are adhered to;

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:
(a) binding corporate rules in accordance with Article 43; or	(a) binding corporate rules in accordance with Article 43; or
(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	(b)standard data protection clauses adopted by the Commission.[1] Those implementing acts shall be adopted 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 the examination procedure referred to in Article 87(2); or

[1] The possibility of also making provision for the sub-processor in Article 42(2)(b) to (d) should be considered, to deal with cloud computing configurations in particular.

(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. (e) codes of conduct examined and recommended by the European Data Protection Board, insofar as the competent supervisory authorities take them into account[1]. [2]
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 or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

[1] Subject to the further discussion of Articles 38 and 58.

[2] Germany would suggest examining whether the participation of third states or international organisations in international data-protection systems (e.g. those of APEC and ECOWAS) can be adopted as a new component under the "appropriate safeguards" listed in Article 42(2). Although these systems are still in the early stages of practical implementation, the draft Regulation should make allowance right away for the significance they may gain in future (cf. also the suggestion regarding Article 41(2)(d) and footnote 2). Provision could for example be made for an international data-protection system to be "recognised by the Commission pursuant to the examination procedure referred to in Article 87(2)" and to function as an appropriate safeguard once it has been recognised.

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 (…) 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[1].
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).	5.	(…) [2]Authorisations on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by the competent authority in the Member State concerned. Authorisations shall be reviewed after the entry into force of this Regulation.

[1] Options for streamlining administration should be examined when developing the consistency mechanism pursuant to Article 57 et seq.

[2] Germany proposes moving the provision on authorisation deleted here to Article 44(2)(i).

	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.	
Article 43 ***Transfers by way of binding corporate rules*** 1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:		*Article 43* ***Transfers by way of binding corporate rules*** 1. A supervisory authority shall in accordance with the consistency mechanism[1] set out in Article 58 approve binding corporate rules, 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 concerned within the controller's or processor's group of undertakings, and include their employees;
(b) expressly confer enforceable rights on data subjects;	(b) expressly confer enforceable rights on data subjects;
(c) fulfil the requirements laid down in paragraph 2.	(c) fulfil the requirements laid down in paragraph 2. .
2. The binding corporate rules shall at least specify: (a) the structure and contact details of the group of undertakings and its members;	2. The binding corporate rules shall at least specify:[1] (a) the structure and contact details of the group of undertakings and the members concerned;

(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;
(c) their legally binding nature, both internally and externally;	(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 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;

(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;
(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;

(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;
(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;
(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;
(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;

(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.
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, after obtaining an opinion from the European Data Protection Board, 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.

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).	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), after an opinion has been obtained from the European Data Protection Board.
Article 44 ***Derogations*** 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:	*Article 44* ***Derogations*** 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:

(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[1] 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
(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 implementation of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's initiative; or .

[1] This adjustment merely concerns the translation of the term "consented" in the German language version.

(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
(d) the transfer is necessary for important grounds of public interest; or	(d) the transfer is necessary for important grounds of public interest[12]; 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

[2] In recital 87, the reference to transfers to competent authorities for the prevention, investigation, detection and prosecution of criminal offences should be deleted, because these do not fall within the scope of the Regulation.
The effects of derogation (d) in conjunction with paragraph 5 need to be examined, in particular with respect to the transfer of data on the basis of court judgments and decisions by administrative authorities of third states, and with regard to existing mutual legal assistance treaties.

(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
(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; 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.	(h) the transfer is necessary for the purposes of <u>overriding</u> 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[1].
	(i) the competent supervisory authority has granted prior authorisation. Authorisation is not granted insofar as on an individual basis, also taking account of points (a) to (h), the data subject has overriding legitimate interests in the data not being transferred. 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[2].

[1] Point (h) needs to be discussed further. In particular, the terms "frequent" and "massive" are unclear.

[2] Public entities should be exempted from this provision, because they are already checked by a state authority, which is itself subject to supervision and involved in procedures of mutual administrative and legal assistance.

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.
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.	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.
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), (c) and (h) <u>and (i)</u> 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 exist[1] in Union law or in the law of the Member State to which the controller is subject. The law of the Member State may establish a public interest that prevents a transfer.
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.	7.	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.
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.	8.	The Commission shall be empowered to adopt (…) the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

[1] Using the word "exist" should make it clear that it is the public interest of the EU Member State being referred to, and not that of the third state.

Article 45 ***International co-operation for the protection of personal data***	*Article 45* ***International co-operation for the protection of personal data***
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:
(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;	(a) develop effective international cooperation mechanisms to facilitate the 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;

(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;
(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.
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 and the supervisory authorities shall take appropriate steps to advance the relationship with third countries, international data-protection systems or international organisations, and in particular their supervisory authorities. (…)

ADDITIONAL COMMENTS

Germany is grateful to the Presidency for the opportunity to submit written comments on Chapter V. We would also like to thank the Presidency for incorporating into the legal text and/or reflecting in the footnotes some of the suggestions from the written German position of 4 March 2013. These suggestions remain valid unless the following comments expressly deviate from them. Scrutiny reservations, unless expressly withdrawn, remain in force.

A. General comments

At present Germany is still unable to endorse Chapter V in its entirety.

The provisions in Chapter V of the draft Regulation perpetuate the system that applies under the existing EU Data Protection Directive 95/46/EC with regard to transfers to third countries.

- Germany welcomes the possibility of transferring data by way of appropriate safeguards, in particular the provisions on binding corporate rules (Article 43 of the draft Regulation), together with the standard data protection clauses or authorised contractual clauses (Article 42 of the draft Regulation). They are not only commercially relevant. Appropriate safeguards, for example, play a major role in the field of research also.

- Safe Harbour currently forms the main basis for data transfers to the USA. However, the Safe Harbour model contains some flaws, especially as regards its effectiveness in terms of both controls and legal protection. In its evaluation report on the functioning of the Safe Harbour of November 2013 the Commission found that improvement was needed because some of the requirements arising out of the Safe Harbour Decision had not been adequately addressed. The Regulation should contain a legal basis for safeguards which are recognised by the EU, which are subject to effective state control and which are acceptable to companies in the respective third country. Germany intends to flesh out its ideas on this point.

- Chapter V was discussed at the informal JHA Council in Athens in January 2014. The Ministers came to the conclusion that the conditions governing data transfer to third countries needed to be examined further and that overall a range of safeguards ought to be flexibly applied. It was still broadly agreed that, while the system of adequacy decisions should be retained, it had to be augmented with further alternatives.

- The question of when, if at all, the publication or communication of data via the Internet can be regarded as data transfer to a third country needs to be clarified.

- Germany would recall its proposal that transfer of data to authorities and courts in third countries should be subject to a notification and authorisation requirement (new Article 42a). The EP also provides for a similar arrangement. The background to the German proposal was the public discussion of the political events in the summer of 2013. The initiative is aimed mainly at increasing the transparency of data transfers – outside the framework of legal and administrative assistance – from companies to authorities in third countries. While Germany is aware of the difficulties that arise for companies owing to legal uncertainties, it also sees the proposal as providing an incentive for a broader dialogue with third countries on data transfers. Germany would be pleased to discuss this proposal further in the DAPIX.

B. Comments concerning Articles 41 to 45

Recital 78

If the market location principle is taken to mean that data may be transferred by the company that is subject to that principle to another company in that (or another) third country only in accordance with the additional requirements of Chapter V, the consequences should first be discussed.

Recital 87

- Germany suggests that, for greater clarity, "necessary for the protection of (…) reasons of public interest" be reworded "**necessary for reasons of public interest**".

- The examples at the end of the first sentence "between competent authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing" should be deleted because they come within the scope of the Directive, not the Regulation.

Article 41

- Paragraph 2, recital 81 (criteria for assessing adequacy)
  The German proposal on taking account of the participation of third countries in international data protection systems should be understood in abstract terms, meaning "the Commission takes into account". It is not a question of every country that is certified under the APEC Cross Border Privacy Rules being automatically regarded as having an adequate level of data protection.

  Germany proposes a new Article 41(2)(d), worded as follows: "**participation in a suitable international data protection system established in third countries or a territory or a processing sector**".

- Paragraphs 2a to 3a, recital 81 (adequacy decision procedure)
  Germany continues to favour EDPB involvement in decisions on adequacy levels in third countries. This would ensure first and foremost that the supervisory authorities, too, could contribute to the procedure with their expertise. The Legal Service informed DAPIX that it would be legally possible to incorporate in the legislative text an obligation for the Commission to obtain a non-binding opinion from the EDPB.

- Paragraph 3a (continued validity of adequacy decisions)
  In Germany's opinion this requires further discussion.

- Paragraph 5
  The paragraph now has a new, autonomous meaning. Germany's reservation (footnote 27) can therefore now be lifted.

Article 42

- Paragraph 5b (continued validity of authorisations)
  The comments regarding Article 41(3a) apply here *mutatis mutandis*.

Article 43

- In the title of Article 43 the words "Transfers by way of" should be deleted since transfers themselves are dealt with in Article 42, with Article 43 regulating only the requirements governing BCRs and their approval.

- Paragraph 1(a) (users of BCRs)
  "Group of enterprises" should be defined.

- Paragraph 2 (content of BCRs)

  Germany suggests adding a point (l) to paragraph 2 as follows: "**the mechanisms for reporting to the 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**". A comparable obligation can be found in standard contractual clauses. Compulsory notification enables the supervisory authority to decide whether to withdraw the authorisation.

- Paragraphs 3 and 4 (specification of criteria, format and procedures by the Commission)

  Here, too, the Commission should obtain the opinion of the EDPB in advance.

Article 44

- Paragraph 1 (derogations)

  BCRs are also "appropriate safeguards" under Article 42. To avoid confusion, an explicit reference should be avoided and the wording should instead be as follows: "In the absence of an adequacy decision pursuant to Article 41 **or** of appropriate safeguards pursuant to Articles 42 **and 43**".

- Paragraph 1(h), recital 88 (legitimate interest of the controller/processor)

To prevent paragraph 1(h) turning into a "super derogation", given that the terms "large scale or frequent" remain unclear, an "**overwhelming** legitimate interest" should be necessary and the obligation to state the facts for the consideration of interests should lie with the processor, not with the data subject. It should therefore properly read "**which override the interests or rights and freedoms of the data subject**". In addition, consideration should be given to further security measures, such as the obligation to obtain authorisation from the supervisory authority

GREECE

Article 40-General principle for transfers

Article 40 refers to the general obligation for the controller and processor to comply with the provisions of this Chapter. We would like to suggest deletion of this Article or its content to be included in recital 78.

Article 41- Transfers with an adequacy decision

In art.41 paragraph 2 (a): We would like to suggest the addition of the following phrase "…***the adequate level of protection of human fundamental rights and freedoms and especially"*** so the the point (a) would read as follows:

(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 ***the adequate level of protection of human fundamental rights and freedoms***, ***and especially*** 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;

In paragraph 6, we would like further clarification on the phrase "*at the appropriate time*", i.e. when time can be appropriate to start consultations and also until that time how absolute the prohibition to transfer data to the third countries is.

In recital 78 and 79 there is a reference to the transfer of data to third countries where it will be carried in full compliance with the Regulation (recital 78) and at the same time the Regulation shall not apply to the international agreements which were concluded by EU and third countries (recital 79). This means that the international agreements EU-third countries (which include data transfers) will not be amended after the entry into force of the Regulation and that will continue to be in force as they were concluded in the first place. In such cases, the international law prevails the community law. What happens in the cases of bilateral agreements, i.e. concluded between EU Member States and third countries?

Two thought approaches are suggested:

1) In these cases, the third countries may have been approved as having the adequate level of data protection within the procedure of Article 31, that means that they provide adequate level for data protection and for the future the art. 41 para 8 applies.

2) If this is not the case, the third countries are binding by the provisions for data protection included in the agreements they have concluded with the EU M-St. Also, in these cases the international law prevails when a confict may arise, so when the Regulation comes into force it does not need any amendment of these bilateral agreements.

We suggest, for reasons of legal certainty and clarity, a provision or recital to be included in order to clarify how the bilateral agreements will be treated after the Regulation comes in force.

Article 42-Transfers by way of appropriate safeguards

In art. 42 paragraph 5: We suggest that the provision which refers to the cases when the appropriate safeguards are not provided for in a legally binding instrument should not be applied in the private sector. Furthermore, we would like to have further clarifications on the circumstances and guarantees where the public sector may use the possibility provided in this paragraph.

Article 43-Transfers by way of binding corporate rules

In art. 43 in paragraph 1 point 9 (a): We would like to suggest the addition of the phrase ***'(alliances) enterprises*** which cooperate (financially) with the controller's or processor's group of undertakings " in order to include the whole range of collaboration in the modern computer society where there is a constant flow of data exchange and also to cover cloud computing.

In paragraph 2: Since there is the explanation in para 1 about the **legally** binding corporate rules, we suggest the addition of the word ***"legally***" in para 2 in the introductory sentence in front of the phrase "…binding corporate rules.." Also, we suggest the addition of word ***"legally***" in point (f).

Article 44-Derogations

In art. 44 paragraph 1 points (d) "public interest", point (f) "vital interests", point (h) "legitimate interests": These phrases need further clarification and we suggest to include it in a recital.

In paragraph 6: For reducing the administrative burden (especially in the public sector) and since the supervisory authority shall be informed about the transfer, we suggest deletion of this kind of obligation for the controller or processor.

Delegated Acts included in arts. 43 and 44: Please see our relevant response sent to you on 9 November 2012 by e-mail.

Article 45-International co-operation for the protection of personal data

We do not have further suggestions on this Article.

SPAIN

General considerations

Chapter V deals with the international transfer of personal data.

There is no doubt that in an increasingly globalised world thanks to, among other things, very sophisticated systems of communication and data transfer, this is a fundamental chapter to ensure the consistence of the whole instrument. Indeed, it would be useless to arrange an advanced data protection system at EU level, if there are not procedures to offer guarantees so that the political boundaries do not constitute a simple mean to evade the protection mechanisms established at a local level.

In relation to the abovementioned, the Regulation establishes in its Article 40 a general principle that ensures that *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.*

Obviously, these mechanisms intend to ensure an adequate protection of privacy in the processing operations that take place once the data have been transferred to third countries, but also to establish the security safeguards required for the subsequent transfers from the receptor countries, to have the minimum security acceptable.

Commentaries on article 40:
We find nothing to object the content of this Article.

Commentaries on Article 41:

In general terms, we accept the wording of this Article, though with the following clarifications:

- As it uses the expression "further authorisation", the first paragraph of this Article seems to envisage that even though there is a decision about the adequacy of the data transfer, an initial authorisation is required. In our view, this is not the case, because what the decisions of adequacy actually allow is the possibility of developing data transfer operations without specific prior authorisation. This is why we propose to amend the wording "further authorisation" for "specific authorisation".

- We believe that the idea of envisaging the possibility of partial adequacy acknowledgements is positive. Nevertheless, when these acknowledgements affect only one "territory", it is unavoidable to consider the political implications (at a foreign policy level) that this might have for the EU, and if the exclusive intervention of the Commission is or is not enough. On this particular aspect we do not propose amendments for the moment, but we reserve the right to do so, later on.

- Concerning the decisions of adequacy, we must understand that they must rest in force *rebus sic stantibus* (argument based on paragraph 8), but there is no mention to the procedure to revise these decisions. This is why we understand that in its due time, these situations should be subjected to thorough analysis, and that it is probable that amendments or additional norms will be required to clarify certain issues that may be aroused (causes of revision, initiative, retrospective effects of the revision, audience to the actors…). At this stage we propose a little amendment in paragraph 5, including the phrase "even though a positive adequation decision has been previously adopted".

- The enumeration and the wording of the aspects to be taken into consideration for the adequacy decisions could be improved (paragraph 2.a). To this effect, we propose an alternative wording.

- Concerning paragraph 2 (b), it is important to assure consistence of our draft regulation with the principle of independence of the supervisory and coherence system, which is not still the case, according to the faculties that the Commission wants to retain in the context of the European Board and in the Coherence Mechanism as well.

- Concerning paragraph 5 it must be taken into account the political impact of such a decision. We accept retaining the wording at this stage assuming that enforcement acts would consider with care the specific political implications in every case.

- The wording of paragraph 6 should also be clarified, because the use of the term "prohibited" is not consistent with the following Articles, as it is already envisaged in paragraph 6. In this sense, we believe it would be more convenient to use the word "restricted".

Therefore, we propose the following amendments:

Article 41

Transfers with an adequacy decision

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.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

   (a) the **level of penetration and consolidation of 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 **the data protection** security measures which are complied with in that country or by that international organisation, as well as **the right to access to justice and the effectiveness and enforceability of the rights,** ~~effective and enforceable rights~~ including **the right to** effective administrative and judicial **action and** redress ~~for data subjects~~, in particular for those data subjects residing in the Union 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

(c) the international commitments the third country or international organisation in question has entered into.

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).

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.

5. The Commission may decide, even though a positive adequation decision has been previously adopted, 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).

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~~ **restricted**, ~~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.

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.

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.

Commentaries on Article 42:

Article 41 was based on the existence of a positive or negative act of the Commission, which behaved as a legitimation or restriction element for transfers. Nevertheless, in certain cases, it might be interesting to carry out some kind of data transfer to a third country when there is no pronouncement of adequacy by the Commission.

For these cases, Article 42 lists a series of alternatives. We are satisfied with them, although we understand that the prior authorisations envisaged in paragraphs 4 and 5 could be replaced by the intervention of a Data Protection Officer, if any, or by the existence of a sufficient certification, in the terms of the certification policy envisaged in Article 39.

Furthermore, we understand that due to the reference that this Article does to Article 41.6, the data transfer through appropriate guarantees should be also applicable when the decision of inadequacy is based on the fifth paragraph of this Article.

Article 42

Transfers by way of appropriate safeguards

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.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

(a) binding corporate rules in accordance with Article 43; or

(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

(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

(d) contractual clauses between the controller or processor and the recipient of the data, authorised by a supervisory authority if there is no data protection officer apointed or valid certification for international transfers, in accordance with paragraph 4.

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.

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**, if the organization lacks of data protection officer or sufficient certification in force,** 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.

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**, if the organization lacks of data protection officer or sufficient certification in force,** 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.

Commentaries on Article 43:

We are globally satisfied with the content of this Article, although we propose a reduced number of amendments to be coherent with some of our general positions in relation to the instrument.
Nevertheless we believe it's important to extent the scope of the binding corporate rules, in order to allow more flexibility for enterprises that have a very close relationship through alliances, or commercial agreements.
Furthermore, the controller or the processor should have the possibility of delimiting the scope of the binding corporate rules within the group of undertakings.
Secondly, we believe that the expression "by electronic means" in paragraph 4 should be suppressed with basis on the technologic neutrality principle, that in our view should inspire the whole regulation.
Therefore, we propose to amend the Article as follows:

Article 43

Transfers by way of binding corporate (partnership) rules

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:

(a) are legally binding and apply to and are enforced by every member within the controller's or processor's defined scope for a group of undertakings or among business partners, and include their employees;

(b) expressly confer enforceable rights on data subjects;

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify:

(a) the structure and contact details of the group of undertakings or business partners, and 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;

(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;

(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;

(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 partner or 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;

(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;

(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings or among the business partners, the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;

(i) the mechanisms within the group of undertakings, or among the business partnerts, aiming at ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the policies 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 or any partner, 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.

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.

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).

Commentaries on Article 44:

This Article operates as the closing clause, as it establishes a series of restricted possibilities for the international transfer of personal data in those cases in which there is no adequacy decision nor the guarantees of Article 42 are applicable.

Somehow, this norm refutes the idea expressed in absolute terms on Article 41, that the international transfer of personal data is forbidden to the countries or institutions affected by the decision, when there is a decision of inadequacy. What happens in these cases is that the transfer will only be possible in the cases established in the Regulation, if it complies with the requirements envisaged for each case.

In general we agree with the content of the Article. However, without prejudice of the details that might arise during the sessions of the working group, we propose the following amendments:

- For the case envisaged in letter e) -defence of legal claims- it seems convenient to also include the legal claims in an administrative procedure, because in great number of cases, these procedures are the initial channel to exercise and defend those claims.

- As regards to paragraph 4, the suppression of letters b) and c) should be thoroughly studied. We therefore reserve our opinion until the Article has been discussed in the Working Group.

- The delegated acts envisaged in paragraph 7 seem to be excessive, as they allow determining essential aspects of the regulation, not just development issues. If it is necessary to fulfil essential aspects of these rules, it should be done in the Article at first.

- As for paragraph 6, in coherence with our position, we understand that the documentation obligations in the terms of Article 28 will take place when they are required according to the amendment we proposed for this Article, that is to say, when there is no Data Protection Officer or sufficient certification in force. The rest cases will be regulated by the general principle of accountability.

Article 44

Derogations

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:

(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

(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

(d) the transfer is necessary for important grounds of public interest; or

(e) the transfer is necessary for the establishment, exercise or defence of legal claims **in an administrative or judicial procedure**; 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

(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

(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.

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.

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.

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.

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**, when it is appropiate according to that Article,** and shall inform the supervisory authority of the transfer.

~~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.~~

Commentaries on Article 45:

Article 45 regulates the international co-operation, and its paragraphs 1.a) and 1.b) envisage the development of mechanisms of co-operation and activities of mutual assistance to ensure the compliance with the respective legislations on data protection.

The text we suggest here is intended to complement and detail these two paragraphs, establishing the conditions by which such agreements and activities may be developed. The model we suggest is taken from the one established for the co-operation of the audit authorities in Directive 2006/43/EC, of 17th May 2006, on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC.

Therefore, we propose adding a paragraph between actual paragraphs 1 and 2, which would become paragraph 2, with the following wording: *"for the purposes of paragraph 1, letters a) and b) the supervisory authorities may exchange information and cooperate in activities related to the exercise of their powers and the tutelage of the rights envisaged in this Regulation"*.

We also propose to add three paragraphs more that regulate the cases, scope and safeguards that should discipline the international co-operation between national supervisory authorities.

Article 45

International co-operation for the protection of personal data

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;

   (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;

(d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, letters a) and b) the supervisory authorities may exchange information and cooperate in activities related to the exercise of their powers and the tutelage of the rights envisaged in this Regulation.

3. Such cooperation may take place as long as:

(a) the competent authorities of the third countries are duly empowered to protect personal data in the specific field o subject;

(b) there are working agreements in the matter based on reciprocity between the competent authorities;

(c) the data transfer to the third country is in accordance with Chapter V of this Regulation.

4. The working agreements referred to in letter b) shall ensure that:

(a) the competent authorities can justify the aim of the cooperation request;

(b) the people employed or previously employed by the competent authorities of the third country that receives the information are subject to professional secrecy;

(c) the competent authorities of the third country can only use the results of the cooperation for the development of duties related to data protection;

(d) if the competent authority of the third country intend to transfer to another party the information received in the field of the cooperation, it shall previously obtain specificific and written consent from the authority that provided the information, unless the transfer is compulsory according to their national law or it has been ordered by a judge and constitutes a necessary meassure to safeguard public interests with regard to:

The prevention, investigation or prosecution of criminal offences.

The supervision, inspection or regulatory duties connected to, even occasionally, the exercise of the official authority within the scope of the agreement.

In that case, there shall be a prior information to the authority that provided the information.

(e) **security, technical and organizative meassures, appropiate for the protection of the personal data against accidental or illicit destruction, accidental loss, alteration, difusion or non-authorized acess and any other illicit processing of personal data are adopted.**

(f) **the request for cooperation from the competent authority of the third country shall be rejected when:**

It affects adversely the sovereignity, security or public order of the Union or a Member State, or

A judicial proceeding has been initiated on the same matters and against the same subjects before the authorities of the Member State.

5. **The Member States shall communicate the Commission the working agreements mentioned in sections 3 and 4 of this article.**

6. 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).

Conclusions:

Chapter V is one of the main pieces of the instrument. Commission's proposal cannot be accepted as is, because it lacks flexibility.

We propose to act through an accountability-based approach, and at the same time giving some more room for manoeuvre to the stakeholders.

Although the core of the approach seems correct, we suggest a certain flexibilization of the supervisory authorities' authorisations and approvals of Article 42, for those cases in which the organization has a Data Protection Officer or a sufficient and in force certification. This is coherent with the general approach of our position, which intends to search for alternative instruments to bureaucratic burdens, by favouring auto regulation and accountability based on the prior safeguards granted by a high level data protection officer model, or alternatively, a solid and clear certification policy.

Additionally we are in favour of extending the scope of the binding corporate rules, in order to give more flexibility for outsourcing. From our point of view these is an important measure requested form different sectors, and especially from the Cloud Computing providers. Moreover, we don't see specific risks in our proposal as long as the main safeguard, approval by the national authority, is retained.

Finally, through various amendments to Article 45 we have tried to define an adequate framework to strengthen the international co-operation at a supervisory authority level, which constitutes one more element of quality and security for the international transfer operations.

The Spanish delegation would like to thank the Presidency for its last proposal regarding Chapter V and Article 18.

Comments on Chapter V: Transfer of personal data to third countries or international organisations

Article 41.2.b)

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 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*

As a principle, the Spanish delegation would not support the approach of establishing requirements that are formally linked to a certain tradition of data protection (the European tradition) that do not exhaust the possibilities of ensuring a high level of protection. There are countries that do not have a Data Protection Authority (or at least, not with the features envisaged in the draft Regulation) and other countries in which the DPA does not have sanctioning powers, which nevertheless have efficient data protection systems. Currently, there are examples of the latter in the EU, and we would not consider that these countries had a weak protection. In sum, we support demanding a high level of protection in third countries that will benefit from an adequacy decision, but we do not believe that the only possibility of ensuring it is through the European model.
Perhaps it would be useful to turn to the language used in the Opinion WP 12 of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, which refers to "some sort of institutional mechanism allowing independent investigation of complaints", and to the fact that "the existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials".

Article 41.3a

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 the Commission* **in accordance with the examination procedure referred to in Article 87(2). (…)**

This paragraph contains a mistake from the original proposal by the Commission. Article 26.4 of the ’95 Directive does not refer to adequacy decisions, but to standard contractual clauses. There is no objection to the idea of Art. 41.3a, it is just that we believe that, being coherent, the reference to Art. 26.4 should be included in Art. 42.5b.

Additionally, we would like to request the Presidency to include Spain in footnote 25, supporting Germany´s comment. The fact that the Comitology procedure does not envisage the possibility of requesting certain bodies such as the EDPB for an opinion does not entail that it is legally prohibited. As we understood it during the last DAPIX meeting, the Council Legal Service considered that establishing the obligation of consulting the EDPB for a non-legally binding opinion before the Comitology procedure was initiated would be consistent with the acquis.

Article 42.2.e) and f)

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

(e) an approved code of conduct pursuant to Article 38; or

(f) a certification mechanism pursuant to Article 39.

We do not object the fact that the appropriate safeguards are provided by codes of conduct or certification mechanisms, but we do think it convenient to make it clear, perhaps in the recitals, that these safeguards must have the same extent as the ones provided by other instruments. We must take into account that, unlike the rest of the instruments, codes of conduct and certifications do not have a contractual (therefore, bilateral) nature. Thus, there are certain elements such as liability and third´s rights, present in the rest of the instruments, which these ones by definition do not envisage.

Article 42.3

3. A transfer based on binding corporate rules or standard data protection clauses as referred to in points (a), (b) or (c) of paragraph 2 shall not require any specific authorisation.

It is not clear to us which would be the rules that will be applied to international data transfers based on codes of conduct or certifications. According to this paragraph, it seems that a specific authorisation will be required. If that is the case, we do not understand why they are included in this provision, because they would belong to the category of international transfer that requires an authorisation. Nevertheless, it seems logical that these instruments, codes of conduct and certifications, should also be exempt of prior authorisation. If not, why mentioning them? An option would be to include them in paragraph 5, but it would also lead to the conclusion that these instruments require prior authorisation.

Article 43.2

2. The binding corporate rules referred to in paragraph 1 shall ***contain a description of*** *at least the following elements:*

We are not sure whether if every letter in this paragraph refers to elements that can be "described". In fact, some of the letters in this paragraph refer to compromises, and we would not want that these compromises are not expressed in the BCR, but in another document, which is simply "described" in the BCR. Therefore, we would modify the wording of paragraph 2 to make this clear, perhaps by including "contain a description **and include**"

Article 44.1.h)

(h) the transfer *which* is not large scale or *frequent*, is necessary for the purposes of legitimate interests pursued by the controller or the processor **which are not overridden by the interests or rights and freedoms of the data subject** and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, *where necessary*, based on this assessment adduced suitable safeguards with respect to the protection of personal data.

Letter h) has a different nature than the rest of the cases envisaged in Article 44.1. While the rest of the letters of this article refer to cases in which an international transfer to a third country without a proven adequate level of protection is allowed based on the own interest of the data subject, or on general interests or third party qualified interests, in this case the processing is permitted because of a mere legitimate interest of the controller. According to Article 6.1.f) and to the new wording of Article 44.1.h), a prior pondering of the controller´s legitimate interest with the data subject´s rights must always be conducted in order to permit a processing based on legitimate interests. Nevertheless, in the present case, as the data are being transferred to a country that has not proved an adequate level of protection, each data transfer entails a risk for the data subject, and the risk is simply justified by an unqualified legitimate interest.

It is true that the provision mentions the need for suitable safeguards. But perhaps these safeguards could be established in instruments already envisaged in other parts of the regulation, such as contract clauses. If this was the case, it would be regulated by art. 42, so article 43.1.h) would be unnecessary.

It could also be adduced that this article refer to transfers which are not "large scale nor frequent". Despite both concepts being utterly undetermined, the fact is that just one single transfer is enough to damage the data subject´s rights.

During the last DAPIX meeting, Spain requested the Presidency to note a scrutiny reservation on this article. Nevertheless, we would support to add a reference such as the suggested in footnote 71. Alternatively or additionally, we would establish an additional safeguard so that it is clear that these international transfers will never affect sensible data of art. 9.

Article 44.5

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. ***Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.***

The Spanish delegation has serious doubts about the scope of this article. Does it refer to the possibility of prohibiting a single controller to transfer personal data? If that is the case, why is it necessary to make this decision by law? Or does it refer to the establishment of a general prohibition to transfer data to a third country as a whole? Is it a "sanction" to a country or to a controller? If that is the case, the provision should be encompassed in the proper chapter. And, anyway, is Article 44 the adequate place to introduce this provision? Until these aspects are clarified, we would like to request the Presidency to note a scrutiny reservation on this article.

Article 45

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;
(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;
(d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, letters a) and b) the supervisory authorities may exchange information and cooperate in activities related to the exercise of their powers and the protection of the rights envisaged in this Regulation.
3. Such cooperation may take place as long as:

(a) the competent authorities of the third countries are duly empowered to protect personal data in the specific field or subject;
(b) there are working agreements in the matter based on reciprocity between the competent authorities;

(c) the data transfer to the third country is in accordance with Chapter V of this Regulation.

4. The working agreements referred to in letter b) shall ensure that:

(a)the competent authorities can justify the aim of the cooperation request;
(b) those employed or previously employed by the competent authorities of the third country that receives the information are subject to professional secrecy;
(c) the competent authorities of the third country can only use the results of the cooperation for the development of duties related to data protection;
(d) if the competent authority of the third country intend to transfer to another party the information received in the field of the cooperation, it shall previously obtain specific and written consent from the authority that provided the information, unless the transfer is compulsory according to their national law or it has been ordered by a judge and constitutes a necessary measure to safeguard public interests with regard to:
The prevention, investigation or prosecution of criminal offences.
The supervision, inspection or regulatory duties connected to, even occasionally, the exercise of the official authority within the scope of the agreement.
In that case, there shall be a prior information to the authority that provided the information.
(e) security, technical and organisational measures, appropriate for the protection of the personal data against accidental or illicit destruction, accidental loss, alteration, diffusion or non-authorized access and any other illicit processing of personal data are adopted.
(f) the request for cooperation from the competent authority of the third country shall be rejected when:
It affects adversely the sovereignty, security or public order of the Union or a Member State, or
A judicial proceeding has been initiated on the same matters and against the same subjects before the authorities of the Member State.

5. The Member States shall communicate to the Commission the working agreements mentioned in sections 3 and 4 of this article.

6. For the purposes of paragraph 1, the Commission **and supervisory authorities** 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).

Comments on Article 18: Right to data portability

2. Where the data subject has provided personal data and the processing, (…) based on consent or on a contract, is carried on in an automated processing system ~~[provided by an information society service]~~, the data subject shall have the right to ~~withdraw~~ **dispose of** these data in a **commonly used format and** to **request the controller or processor to** transmit them into another automated processing system without hindrance from the controller from whom the personal data are withdrawn, **without prejudice to Article 17**.

The current version of this article does not clearly envisage two cases that in our opinion should be included within the scope of the right to data portability: the right of a data subject to request a controller to directly transmit the data to another controller (for example, a user requests Facebook to transmit all his or her pictures to Picasa), and the right to request the first controller to erase those data after transmitting them to the second controller (for example, a user requests Facebook to erase his or her pictures and transmit them to Picasa). In order for the right to data portability to answer to these cases, we propose the above wording for Art. 18.2.

FRANCE

Chapter V - Transfer of personal data to third countries or international organisations

By way of a general comment on this Chapter, the French authorities would emphasise that while we agree that the decisions on adequacy adopted under Directive 95/46 before the entry into force of the package proposed by the Commission should remain in force, we are however opposed to the European Commission being empowered to adopt "negative" decisions declaring that a third country, a territory or a data processing sector within that third country, or an international organisation does not ensure an adequate level of data protection.

Besides the diplomatic consequences, which are not to be underestimated, such decisions would force Member States to renege on existing agreements with third countries, without any possibility of renegotiating them.

In the same vein, the French authorities wonder what is to happen to the bilateral and multilateral agreements concluded by Member States with third countries or international organisations on the subject of data protection, or which secondarily organise transfers of data (tax treaties for example), insofar as no provision of the Regulation mentions their fate (recital 79 alone preserves international agreements concluded between the Union and third countries regulating the transfer of personal data).

We **therefore enter a general reservation on Chapter V,** and request that at the very least a grandfather clause be inserted preserving international agreements concluded by Member States, along the lines of Article 41(8), which already provides for the decisions on adequacy adopted by the Commission under Directive 95/46 to remain in force.

Article 40 - General principle for transfers

At first sight, the French authorities consider the usefulness of this Article to be questionable.

Indicating in a main Article that any transfer of data must comply with the rules laid down by the Regulation seems unnecessary.

We feel that the only useful part of this Article is the last phrase: "*including for onward transfers of personal data … to another third country or to another international organisation*".

The French authorities would nevertheless stress that this phrase, which seems to refer to the principle of "originator control", is clumsily expressed. It is not realistic to burden a Member State with a responsibility in such general terms regarding the subsequent use of data that it has transferred to a third country or an international organisation, nor to burden that third country or international organisation with the obligation to comply with European data protection rules (this would mean applying the Regulation outside the EU, something that would be difficult to implement and enforce). The obligation is either too general, or it is difficult or indeed impossible to enforce.

If it is indeed the principle of "originator control" that the Commission intended to anchor in this Article, the French delegation would in this case suggest using the conventional wording on subsequent transfer, based on the necessity of obtaining prior agreement from the controller at the origin of the first international transfer before being able to proceed with a subsequent transfer. We would thus suggest the adoption of the following wording:

"In any transfer to a third country or an international organisation, the controller or processor shall require the recipient of the transfer to obtain the prior consent of the controller at the origin of the data transfer before any subsequent transfer."

The French authorities would also draw attention to their previous comments on the need to clarify the sharing of responsibility between the controller and processor. This also needs to be clarified with regard to international transfers.

In terms of the transfer of data to international organisations, the French authorities would appreciate clarification as to which international organisations are covered (only those of which the EU is a member or any international organisation of which at least one Member State is a member?), as well as of the relationship between the provisions of this Regulation and the specific data protection rules of such organisations.

Finally, the French authorities also feel that the relationship between this Article (and this Chapter more generally) and the rules applicable to archives needs to be clarified, as does that between these measures and the rules on reusing information from the public sector, envisaged in the ongoing revision of Directive 2003/98. In addition, the French authorities would stress that there are specific rules for the dissemination of archives, in particular public archives, and notably with regard to the rules concerning national treasures, that need to be taken into account in this proposal for a Regulation.

Article 41 - Transfers with an adequacy decision

Regarding paragraph 2, the French authorities are in favour of the existing system based on Directive 95/46 being maintained.
Nevertheless, we would point out that the current adequacy procedure has not led to the adoption of many adequacy decisions, and could express our misgivings concerning the possibility, opened up by the proposal for a Regulation, of limiting adequacy decisions to certain sectors (in point (a) "*both general and sectoral*" and in paragraph 3). We therefore call for the deletion of the words "*both general and sectoral*" from paragraph 2 and of "*a territory or a processing sector*" from paragraph 3.
By way of example, the French authorities would highlight that the United States do not currently benefit from a single adequacy decision.

Moreover, the French authorities wonder about the desirability of adopting formal criteria rather than obligations to achieve certain results (for example adopting the criterion of effective protection of rights rather than that of the existence of an independent supervisory authority). In any event, we feel that Member States should be involved in the adoption of adequacy decisions, as is currently the case in the framework of the committee procedure of Article 31, and that Article 41 should make provision for Member States to evaluate the data protection level of a third country or international organisation, if need be by submitting their evaluation to the European Commission.

Concerning paragraph 5, and as indicated in the general comments on Chapter V, the French authorities would stress that it is out of the question for the Commission to be empowered to adopt "negative" adequacy decisions. We therefore call for the deletion of this paragraph and the following two paragraphs (paragraphs 6 and 7), which, aside from the diplomatic consequences not to be underestimated, would prevent all data exchange with a country, territory or international organisation that is subject to such a decision until the Commission "*at the appropriate time ... enter[s] into consultations with a view to remedying the situation resulting from the Decision made*".

In any event, we would also point out that the end of the first sentence of paragraph 5 appears vague and restrictive. The specification concerning "*those data subjects residing in the Union*" is incomplete, unjustified and complicates the text in an unhelpful fashion. The French authorities therefore feel it would be better to delete it.

Finally, we feel that public security, defence or national security, which are excluded from the scope of the Regulation **and** from the scope of the proposal for a Directive, should not be mentioned.

Article 42 - Transfers by way of appropriate safeguards

The French authorities have reservations about the "standard clauses" referred to in paragraph 2(b), and oppose the possibility for such standard clauses to be adopted unilaterally by the European Commission without the participation of Member States. The current wording is very imprecise as regards the content of clauses of this type and the way they will be applied.

Regarding point (c) of the same paragraph, the French authorities would like Member States to be involved in the Commission's work on standard clauses.

The French authorities would also like the wording in paragraph 5 to be clarified, in particular regarding transfers which "*substantially affect the free movement of personal data within the Union*".

Finally, in the same paragraph, the French authorities would also ask that the concept of "*administrative arrangements*" be clarified.

We are in favour of the first paragraph of Article 34 being deleted, further to the addition of the new paragraph 6, which, as indicated in footnote 476, has been moved from paragraph 1 of Article 34 of the initial version of the proposal for a Regulation.

The French authorities would once again highlight however that the wording of this paragraph should be amended insofar as it is not a question of "mitigat[ing] the risks" but of "***ensur[ing] that the necessary measures*** to minimise the risks" have been taken.

In addition, the French authorities also have reservations about the fact that this paragraph applies only to data transfers to third countries.

Article 43 - Transfers by way of binding corporate rules

The French authorities wonder whether these corporate rules concern only the private sector or whether they are also applicable to public establishments responsible for commercial activities.

The French authorities would like the words "at least" to be deleted from the introductory sentence of paragraph 2. This wording suggests that the binding rules could specify other points, without mentioning what these might be. This lack of precision thus creates a legal uncertainty which has no place in a Regulation.

In point (f) of the same paragraph, in line with the general comments already made, the liability of the processor of the body which receives the transfer should be made clearer, as should the provision's applicability with respect to the processor.

Article 44 - Derogations

The French authorities enter a specific scrutiny reservation concerning this Article as regards its application to archives, in particular given the specific rules that govern the dissemination of public archives, including rules on national treasures. We would emphasise in particular that we have misgivings for example about the concept of a "*set of transfers*" (in paragraph 1) and "*entire categories of ...data*" (in paragraph 2) and about the relationship between the proposal for a Regulation and the proposal for a Directive on the re-use of public data, which is currently undergoing revision and whose scope encompasses archives.

We feel that the concept of "*important grounds of public interest*" used in paragraph 1(d) is inappropriate. While "*public interest*" is a well-known concept, adding a distinction based on a subjective evaluation ("important") makes the concept ambiguous and difficult to implement.

In addition, we would draw attention to our reservation regarding the use of delegated acts and assert that it is not acceptable for this concept to be defined through a delegated act, as provided for in paragraph 7. If necessary, it would be a matter for Member States to participate in defining this concept.

For the same reason, paragraph 5 should also be made clearer to specify the meaning of the word "*or*" ("***or*** *in the law of the Member State*").

The French authorities would also point out that there is a contradiction between paragraphs 5 and 7 of this Article.

Still on the subject of the concept of public interest, recital 87, which deals with this issue in terms of combating tax fraud, should be amended. We would like this recital, which specifies by means of examples the grounds of public interest justifying the application of derogations from the conditions of transfers to third countries provided for in Articles 41 and 42, to explicitly mention administrative assistance, whether it is on request, spontaneous or automatic.
We are particularly concerned about the relationship of the proposal for a Regulation, and in particular its Chapter V, with Directive 2011/16/EU on administrative cooperation, which entered into force on 1 January 2013, as well as with the information exchange clauses of bilateral tax treaties on the basis of which data flows take place in automatic exchanges.

In points (g) and (h) of paragraph 1, the French authorities would like some clarification concerning the concept of "legitimate interest(s)".
In any event, we would stress that we would like the balance of Directive 95/46 to be preserved in point (h), as for Article 6(1)(f).

We would once again highlight the need to make the sharing of responsibilities between the controller and the processor clear in paragraph 6.

Article 45 - International cooperation for the protection of personal data

The French authorities draw attention to their general comments and in particular the need to introduce a grandfather clause preserving the international (multilateral and bilateral) agreements of Member States concluded before the entry into force of this proposal for a Regulation.

The French authorities therefore propose the addition of a new Article 89a:

"Relationship with previously concluded international agreements

International agreements concluded by Member States and the Union before the entry into force of this Regulation shall remain applicable until they are amended, replaced or repealed."

The French authorities would also like to see some more details on the role of data protection authorities. More specifically, clarification is needed regarding the relationship between the role bestowed on national data protection authorities by this Article and the role of national legislators. As it stands, the Article in no way addresses potential differences of opinion or indeed conflicts between a national data protection authority and the legislator of its Member State as regards the appropriate measures mentioned in this Article.
The French authorities would also like a legal analysis on potential conflicts between the decisions of the supervisory authority and the legislation of the Member State (in particular as far as ratified international agreements are concerned).

ITALY

Article 40 (General principle for transfers)

This is a general clause establishing the principle of conditional transfer of personal data to third countries or international organisations, thereby providing a systematic conceptual framework.

Our delegation accordingly welcomes this Article, although it feels that consideration should be given to introducing into the text of the proposal for a Regulation (in Article 4) a definition of "transfer" of personal data (in the light of the case-law of the Court of Justice in the *Lindqvist* case, the substance of which could be referred to in a recital). In particular, we believe that there is a need to clarify whether the "transfer" referred to in Chapter V should not include cases where an individual "loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person ("the hosting provider") who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country".

Furthermore, although the text of Article 40 is taken from the directive currently in force (Article 25(1)), we propose that the phrase "*or are intended for processing after transfer*" should be deleted, since the concept is already enshrined in the Article itself and this wording may be misleading for the purposes of applying the rules.
The general principle established in this Article also applies to onward transfers (from the third country of first destination to another third country or another international organisation), which is to be welcomed.

In this connection, our delegation believes that the phrase "*subject to the other provisions of this Regulation*" should be taken to mean that all the conditions governing the processing of the data initially transferred shall also apply to the processing of the data subject to such onward transfers, and in particular that the aims of the processing for which such onward transfers take place shall be compatible with those of the processing for which the initial transfer took place (cf. the comments relating to Article 45).
We appreciate the reasons why "international organisations" have been included among the potential recipients of personal data, but we feel that the nature of such "international organisations" should be clarified, in order to determine, for example, whether this Article is referring to bodies recognised on the basis of international treaties, or to other bodies such as NGOs.

This issue is also linked to the reference, in recital 79, to international agreements between the European Union and third countries, to which the Regulation is "without prejudice".
Such a matter cannot be relegated to a recital, and should be dealt with in a specific provision of the Regulation.
In any case, it would appear necessary to provide for a linkage mechanism and to indicate a time-frame within which compliance of the existing agreements with the adequacy principles referred to in the Regulation must be verified (cf. the reference to the elements to be considered when assessing "adequacy", as listed in Article 41(2)). A similar principle is established in Article 60 of the proposal for a Directive, with regard to agreements between EU Member States and third countries in the field of judicial cooperation in criminal matters.

Article 41 (Transfers with an adequacy decision)

Paragraph 1: the mechanism for assessing adequacy is based on a decision taken by the European Commission alone, in the light of the criteria laid down in paragraph 2.
However, our delegation believes that specific provision should be made for the involvement of the European Data Protection Board, in accordance with the mechanism currently in force as laid down in Article 30(1)(b) of Directive 95/46/EC, so as to ensure that the authorities responsible for supervising the implementation of the Regulation can make their own contribution.
Moreover, the reference to "*processing sector"* (also to be found in paragraph 3) is unclear, particularly as regards the criteria which should be used to define such processing "sectors" and the mechanisms which would govern any onward transfers. For example, let us imagine that a transfer to a third country "*processing sector"* is authorised. Could such data then be transferred onwards (without prejudice to the other conditions) to an entire third country, or only to a similar "*processing sector*" in that third country?
Paragraph 2: the list of criteria for assessing adequacy cannot be exhaustive. We therefore propose that the words "*in particular*" be inserted at the end of the first sentence, to indicate the possibility of taking other criteria into consideration (bearing in mind also the involvement of the European Data Protection Board).
Paragraphs 5 and 6: we have reservations, including on political grounds, about whether a decision on non-adequacy should be taken by the Commission, and about the possible consequences of such a decision.

Furthermore, the relevant provisions in paragraph 6 (which prohibits the transfer of data in the event of a decision on non-adequacy, but then allows it under the conditions laid down in Articles 42-44) appear to lack consistency. We therefore propose that the paragraphs in question be deleted from Article 41.

Article 42 (Transfers by way of appropriate safeguards)

Paragraph 1: we welcome the fact that provision has been made for legally binding safeguards in the absence of an adequacy decision by the Commission.
The clause in paragraph 5 introducing the option of recourse to instruments that are not legally binding therefore appears to contradict the aim of offering effective protection, and it is particularly difficult to see how it could be applied by public entities.
Paragraph 5: as we have already indicated, a weak clause such as that contained in this paragraph does not appear to be compatible with the binding nature of all the other instruments used to provide adequate safeguards for transfers of personal data to third countries. Moreover, "administrative arrangements" is an exceedingly vague term and could lend itself to differing interpretations.
The additional conditions specified in recital 83 for using such instruments that are not legally binding are insufficient and, as it stands, we propose that this paragraph be deleted apart from the last sentence (which allows the supervisory authorities to maintain and review any ad hoc authorisations already granted on the basis of Directive 95/46/EC, thereby avoiding a legal vacuum).

Article 43 (Transfers by way of binding corporate rules)

Paragraph 1: this provision aims to provide a legal basis for the use of "*binding corporate rules*" (BCRs) in accordance with the procedure that has been developed independently over the last few years by the EU's supervisory authorities. Our delegation can therefore support it.
Paragraph 2: this provision is to be welcomed insofar as the list of criteria and requirements applicable to BCRs is to be understood as being non-exhaustive ("*at least*"). There may in fact be additional criteria and circumstances that the European Data Protection Board and the individual authorities deem it necessary or appropriate to include before authorising a transfer.

Paragraphs 3 and 4: we are firmly opposed to the use of delegated and implementing acts to specify the criteria and requirements laid down in paragraph 2 and the procedural formalities.
Such matters should preferably be left to the European Data Protection Board, following the practical experience gained over the last few years in analysing and approving BCRs.

Article 44 (Derogations)

Paragraph 1: the Italian delegation welcomes the description of the derogations provided for in this paragraph, but wishes to stress that the application thereof can only be subject to a restrictive interpretation since such provisions by their very nature depart from the general principles laid down in the preceding Articles of this Chapter.
More specifically:
Point (d): the reference to "important grounds of public interest" is too broad; as we have pointed out on a number of occasions, there is a need to clarify what is meant by "public interest", possibly by introducing elements from recital 87 into the text and incorporating the wording used in Article 26(1)(d) of the Directive currently in force.
In view of the restrictive interpretation that must be placed on all the provisions contained in paragraph 1, it is also necessary to specify that, even in this case (as well as the cases provided for in points (g) and (h)), the derogation cannot apply to mass, repeated and structural transfers of data.
Point (h): the question of whether the legitimate interests pursued by the controller should prevail over those of the subject cannot be decided by the controller himself; at the very least, the transfer should not take place before the supervisory authority has been informed, as stipulated in paragraph 6.
We also propose that the phrase "*where necessary*" should be deleted, since these are transfers carried out in residual circumstances (see our general comment on paragraph 1) and therefore, in any case, subject to particular restrictions.
Paragraph 3: we feel that the list of criteria that the controller is required to take into consideration when assessing the appropriateness of the transfer is incomplete.
Paragraph 4: we propose adding point (a) to the list of conditions that do not apply to processing carried out by public entities in the exercise of their public powers, in line with the provisions of Article 7(4) of the proposal for a Regulation.
There can be no doubt that the exercise of a public power is difficult to reconcile with the requirement of freedom of consent, and constitutes a "*significant imbalance*".

Paragraph 6: Concerning the reference to point (h) of paragraph 1, we believe that the supervisory authority should be provided with the information prior to the transfer, as an additional safeguard. We therefore propose that the last sentence of paragraph 6 be amended as follows: " [...] *and shall inform the supervisory authority before the transfer*".

Paragraph 7: our delegation requests that this paragraph be deleted on the grounds that it is questionable that the Commission should be given the power to determine, by means of delegated acts, what may count as "*important grounds of public interest*"; the "*appropriate safeguards*" mentioned in connection with point (h) of paragraph 1 could be better defined if the European Data Protection Board were involved.

Article 45 (International cooperation)

Paragraph 1, point (b): There should be more precise definitions of notification, complaint referral, investigative assistance and information exchange. There should also be clarification as to whether "investigative assistance" also includes the possibility of on-the-spot inspections; judging by the provisions of Article 56, this would appear to be the case but, if so, there should be an explicit reference to that Article at this point in the text.
As far as the Spanish delegation's proposal is concerned (DS 1038/13), we welcome the attempt to provide greater clarification of the mechanisms for cooperation between the supervisory authorities, even though this aim does not appear to have been fully achieved in the non-paper.
For example, there is a difference between paragraph 2, which refers to the "supervisory authorities", and the subsequent paragraphs, which contain references to the "competent authorities".
At all events, we agree with the principle established in paragraph 2, which aims to give tangible effect to the possibility that the supervisory authorities involved in a specific investigation or a specific case may exchange relevant information, including personal data, without infringing the confidentiality rules to which they are subject. However, in order for such cooperation to be effective, specific reference should be made to Articles 52, 53 and 56 of the proposal for a Regulation, which contain useful provisions to that end.
Lastly, with regard to paragraphs 3 and 4 of the Spanish delegation's non-paper, it might be more appropriate to use the provisions proposed therein for regulating the onward transfers of data mentioned in Article 40 – for which no rules of any kind have been laid down in the proposal for a Regulation – and include them in an additional, specific Article.

LUXEMBOURG

These comments are without prejudice to any further comments made in subsequent negotiations.

The general remarks made in earlier written comments remain valid, notably with regard to the respective allocation of obligations and responsibilities between controllers and processors that needs to be clarified for chapter V as well.

Detailed comments

Article 41 – Transfers with an adequacy decision

Luxembourg wonders what added value the establishing of "black lists" by the Commission brings, particularly since such decisions of "non-adequacy" will be without prejudice to articles 42, 43 and 44. Luxembourg therefore suggests deleting paragraphs 5, 6 and 7.

Article 43 – Transfers by way of binding corporate rules

Luxembourg strongly supports this article and underlines the necessity that existing approved BCRs should remain valid. A broader scope could be envisaged for business partners or joint ventures that are not groups of undertakings.

The consistency mechanism referred to in paragraph 1 needs to be as unbureaucratic as possible in order for the approval of BCRs to be efficient – possibly consultation of the European Data Protection Board is sufficient. The supervisory authority of the main establishment of the controller or processor shall be solely competent for negotiating the BCRs and for securing approval from other relevant data protection authorities.

Article 44 – Derogations

In paragraph 1, a reference to Article 43 should be added: also in the absence of BCRs, transfers may be possible if the necessary safeguards are in place.

In paragraph 1 (d), Luxembourg prefers « grounds of public interest » (delete « important ») which is agreed legal language.

80 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. The existence of mutual binding obligations of professional secrecy, such as the professional secrecy of the medical and legal professions, or binding special sectoral legislation which protects the interests of data subjects, such as common in the financial sector, may also be used.

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40

General principle for transfers

(...)

Article 41

Transfers with an adequacy decision

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.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to 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;

   (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

   (c) the international commitments the third country or international organisation in question has entered into.

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, if the country, international organisation or processing sector requests the Commission to do so.. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). The Commission will request an opinion of the European Data Protection Board prior to its decision.

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.

5. The Commission may repeal a decision, referred to in paragraph 2 if the Commission finds that the third country, (…)territory or processing sector within that third country, or the international organisation concerned does not ensure the adequate level of protection within the meaning of paragraph 2 of this Article any longer. The Commission will take into account, whether 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 any more. The Commission will request an opinion of the European Data Ptotection Board prior to its decision.

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.

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.

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.

Article 42

Transfers by way of appropriate safeguards

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.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, (…), by:

   (a) binding corporate rules in accordance with Article 43; or

   (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

   (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

   (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4, or

(e) mutual binding obligations of professional secrecy or existing sectoral legislation which offers special protection to the interests of data subject between the controller or processor and the recipient of the data in the third country, territory or processing sector thereof or international organisation.

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.

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.

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 legal 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.

6 The controller [or the processor as the case may be][1] shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to mitigate the risks involved for the data subjects where a controller [or processor] adopts contractual clauses as provided for in point (d) of paragraph (2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in paragraph (5) for the transfer of personal data to a third country or an international organisation[2].

Article 43

Transfers by way of binding corporate rules

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, 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;

   (b) expressly confer enforceable rights on data subjects;

   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify or give a general description of:

   (a) the structure and contact details of the group of undertakings and 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;

   (c) their legally binding nature, both internally and externally;

[1] BE suggested deleting the reference to the processor.

[2] Moved from paragraph 1 of Article 34. DE reservation on the appropriateness of prior authorisation as a tool in this context.

(d) the general data protection principles, in particular purpose limitation, including the purposes which govern further processing, 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;

(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;

(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;

(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;

(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;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules, such as auditing;

(j) the mechanisms for reporting and recording changes to the policies 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.

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.

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).

Article 44

Derogations

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:

(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

(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

(d) the transfer is necessary for important grounds of public interest; or

(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

(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

(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; or

(i) a prior authorisation pursuant to Article 34, paragraph 1, has been issued for the transfer

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.

4. Points (b), (c), (h) and (i) 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. Member State law may designate a public interest of special importance which opposes data transfers to recipients outside the European Union, the European Economic Area, or outside third countries, territories or processing sectors thereof or international organisations that have obtained an adequacy decision pursuant to Article 41.

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. 7.(…)

Article 45

International co-operation for the protection of personal data

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;

(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;

(d) promote the exchange and documentation of personal data protection legislation and practice.

2. (…)

AUSTRIA

Austria appreciates the opportunity to make written comments. As the Austrian delegation was unable to attend the meeting on 21 January 2013 due to last minute flight cancellations, the following comments go into some detail.

With regard to Article 41:
At first sight, the term "processing sector" appears problematic. Without further explanation, it is unclear what the term covers. What is more, it could be argued that a "processing sector" per se will usually be unlikely to have legal protection and sanctioning mechanisms as effective as those available to state structures. In light of the above, the question arises as to whether an adequacy decision concerning only one sector which takes no account of the state (and rule of law) context can really be plausibly justified and implemented.

Furthermore, in Article 2(a) we would ask whether reference should not also be made to the general data protection principles of Article 5 (in any case those of (a) to (e)). This would also correspond to the fundamental idea behind the 1997 paper by the Article 29 Working Party, which provided guidelines for evaluating adequacy. In addition, the general human rights situation in the relevant third country (in particular with respect to freedom of expression or freedom of the press) should also be taken into account.

In addition, Austria supports the comments in the draft report by MEP Albrecht regarding the introduction of a new paragraph 4a. It seems entirely appropriate for the relevant adequacy decisions to be evaluated regularly, so that any possible developments running counter to paragraph 2 can be corrected. The proposed paragraph is worded as follows:
"The Commission shall, on an ongoing basis, monitor developments that could affect the fulfillment of the elements listed in paragraph 2 in third countries and international organisations concerning which […] pursuant to paragraph 3 has been adopted."

Given that the EU legal framework is being substantially amended, the benchmarks against which previous adequacy decisions are to be measured are also changing. Consideration should therefore be given to setting an absolute time limit in paragraph 8, within which the Commission's previous decisions would have to be reviewed using the Regulation's amended benchmark.

With regard to Article 42:

Here too reference should be made to the general data protection principles of Article 5, which form an important benchmark in the given context. To this end, the following could be added to the end of the first paragraph: "*having regard in particular to the general principles as set out in Article 5."*

It is not clear what further safeguards there might be beyond those listed in paragraph 2. The most likely case we can think of is where data are transmitted only in pseudonymised form, i.e. with personal references encrypted. In the interests of legal clarity it is imperative that an effort be made to draw up an exhaustive list.

A literal interpretation of paragraph 6 (= originally Article 34(1)) regarding the sub-case of Article 42(2)(d) creates the impression that "double authorisation" is needed from the supervisory authority, namely authorisation of the contractual clauses as such pursuant to Article 42(4) and in addition prior consultation pursuant to Article 42(6). This begs the question as to whether the latter is in fact desired or whether it is not excessive.

With regard to Article 44:

It is unclear here how the term "appropriate safeguards" in paragraph 1(h) relates to the "appropriate safeguards" in Article 42(2). While Article 42(2) makes provision for the supervisory authority to grant authorisation on an individual basis where there are no general previously validated rules, in Article 44(1)(h) it is enough merely to weigh up the interests of the controller and so no checks by any public authority are required. This completely undermines the logic of the entire system for the movement of data abroad and should therefore be rejected.

In paragraph 2, the last part of the sentence is unclear because it is not sufficiently clear who is meant by "recipient". It could be directed at cases of representation (by lawyers for instance). What is important is that the final recipient of the personal data must be able to prove the requisite legitimate interest.
In paragraph 7 it must in any event remain the responsibility of Member States themselves to determine what constitutes public interest (in keeping with paragraph 5).

With regard to Article 45:
The scope of this article is unclear. For instance, international mutual assistance pursuant to paragraph 1(b) could arguably take place only on the basis of an agreement concluded by the EU or Member States. The provision is however directed in this case at the European Commission and supervisory authorities. Appropriate clarification is needed here.

POLAND

GENERAL REMARKS:

Art. 40 – 45

It must be noticed that 41 speaks about transfer made to the third country, its territories or processing sectors, as well as about international organisations. The other Articles of Chapter V however mention only the third country and international organisations. Due to the fact that the term 'processing sectors' is very unclear and nowhere defined, it is advised to remove it from art. 41(1) and other paragraphs respectively.

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40

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.

Remark:

By comparison, unlike in case of agreements concerning PNR (Passenger Name Record), the scope of data to be transferred to a third country/international organisation is not specified. Perhaps Art. 40 should state, at least in general terms, the purpose of data transfer.

Article 41

Transfers with an adequacy decision

1. A transfer may take place where the Commission, after consulting the European Data Protection Board**,** 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.

2. When assessing the adequacy of the level of protection, the Commission shall take into account the following elements:

   (a) the rule of law, access to justice, international human rights norms and standards, 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;

   (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

   (c) the international commitments the third country or international organisation in question has entered into.

3. (…). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

4. The implementing act shall specify its territorial application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

4a. The Commission shall, on an ongoing basis, monitor developments that could affect the fulfilment of the elements listed in paragraph 2 in third countries and international organisations concerning which implementing act pursuant to paragraph 3 has been adopted.

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).

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.

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.

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.

Remarks:

Art. 41 para. 1 European Data Protection Board is a panel of experts that, owing to its independence and know-how, can contribute to consistent application of data protection law.
As it pertains Art. 41(2), the phrase 'shall give consideration to the following elements' should be replaced with the words 'shall take into account the following aspects'; stronger wording

Art. 41 para 2a It seems consistent to bring para. 2a in line with recital 81 of the Preamble.
Art. 41(3) should be merged with Art. 41(1) as they overlap with each other. The sentence: 'Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)' should be moved to para 1.
Art. 41 para 4a Following the draft report on the proposal for a regulation by Jan Philipp Albrecht (European Parliament) it would be advisable to insert a paragraph 4a concerning the monitoring of the level of protection of personal data afforded by a third-state or an international organisation. Only systematic monitoring of developments in third countries and international organisations provide factual basis for a decision on the absence an adequate level of protection reffered to in para 5.

Article 42

Transfers by way of appropriate safeguards

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.

1a. Those appropriate safeguards shall, at least:
(a) guarantee the observance of the principles of personal data processing as established in Article 5;
(b) safeguard data subject rights as established in Chapter III and provide for effective redress mechanisms;
(c) ensure the observance of the principles of privacy by design and by default as established in Article 23; (d) guarantee the existence of a data protection officer pursuant to Section 4 of Chapter IV.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

(a) binding corporate rules in accordance with Article 43; or

(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

(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

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

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.

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.

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.

Remarks:

In order to enhance the level of personal data protection, the introduction of additional safeguards shall be considered.

Article 43

Transfers by way of binding corporate rules

No changes proposed.

Article 44

Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer (…) 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

   (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

   (d) the transfer is necessary for important grounds of public interest; or

   (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

(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

(h) (…)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. (…)

4. Points (b), (c) and (…) 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.

6. (…)

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.

Remarks:

Art. 44(1e) is vague and requires clarification, as it may lead to transferring of personal data for the purpose of brining copyright claims.
(Art. 44 (1h)) the criterion put forward in point h) is too vague and runs against the principle of legal certainty. Therefore, point (h) of paragraph 1 should be removed and, consequently, paragraphs 3, 4, and 6 need to be adapted as well.
Art. 44 para 1 With regard to paragraph 1, the words ‘set of transfers’ should be erased in order to unify the terminology used in Chapter V, as well as to avoid any doubts as to whether the data subject is to give one consent to the set of transfers or to each of them.

Article 45

International co-operation for the protection of personal data

Remarks:

Article 45 comprises a list of non-legally binding obligations. It seems worth to consider the insertion of art. 45 or a substantial part of it in the recitals.

Data transfers

Issue of the recipient: We would like to draw your attention to the unclear meaning of the term "recipient" in Chapter V. Given the fact that the current definition of the recipient in the Article 4 point 7 states: *'recipient' means a natural or legal person, public authority, agency or any other body other than the data subject, the data controller or the data processor to which the personal data are disclosed* (…),we have doubts as to whether transfers of data to entities other than the recipient, that is, *inter alia*, data processors, are covered by the provisions of Chapter V. In the Polish opinion clarification of this issue is very important. Maybe, for the sake of clarity, it would be good to delete all the references to a "recipient" in Chapter V?

Article 41

Article 41 paragraph 3a: In our opinion, the issue of the decisions recognising adequacy which have been already adopted is very important. It seems that after the entry into force of the regulation the decisions should be reviewed. However, we should not act too hastily in this regard. The overview of the decisions on adequacy could be gradually carried out by the European Commission.

Article 41 paragraph 4a: Third countries and international organisations whose adequacy has been recognised should be monitored, as it is necessary to ensure that the European Commission may decide that particular country/organisation no longer ensures an adequate level of protection.

Article 41 paragraph 5: every decision of the European Commission should be preceded by an opinion of the European Data Protection Board. Poland supports the European Commission being entitled to adopt "negative adequacy findings". In our opinion it will be a factor motivating third countries to introduce higher data protection standards.

Article 42

Article 42 paragraph 1: We support prior authorisation for the transfer by the DPA as a basis for data transfers to third countries, however the question is whether the relevant provision should be included in Article 42 or Article 44, with the latter option being more preferable.

Article 42 paragraph 2 points e and f: We strongly support the idea of self-certification. However, approved codes of conduct and certification mechanisms are not legally binding instruments. Therefore, we can agree to keep them in this paragraph only if it is clarified that they do not constitute a separate basis for data transfers, i.e. a controller or a processor needs to obtain prior authorisation from the competent DPA in accordance with Article 42 paragraph 5, in order to transfer data on the basis of Article 42 paragraph 2 points e and f.

Article 42 paragraph 5: an administrative arrangement, in some jurisdictions, including Polish, has a certain legal meaning and is one of the defined legal instruments. We would like to clarify what this term means for the purposes of the general regulation in a recital.

Article 42a

Poland supports the introduction to Chapter V of the draft regulation of an additional Article 42a (as submitted in document 12884/13). We will support any solution that would allow the Member States to regain control over their citizens' personal data transferred to third countries. Instruments adopted by the Member States should aim to restore the confidence of citizens which has been impaired, *inter alia*, due to media reports regarding PRISM and other mass surveillance programs.

Article 43

Poland supports the regulation of binding corporate rules in the general regulation. We are in favour of keeping Article 43 paragraph 3 in the text. The European Commission has vast experience regarding BCRs, which we should make proper use of.

Article 44

Article 44 paragraph 1 point h: We are in favour of deleting this paragraph. In our opinion, it reduces the level of protection of personal data in comparison to the level of protection of Directive 95/46. The legitimate interest of a data controller or a processor should not constitute a basis for transfer of personal data to third countries.
If Article 44 paragraph 1 point h will not be deleted, we would like "where necessary" to be deleted from the penultimate line of this article.

Recital 87: We support the changes made to this recital, which allow member state law to prohibit the transfer of data to a third country or an international organization due to a public interest recognised in the EU.

Article 44 paragraph 5: Poland believes that this a crucial paragraph . With regard to the first sentence - it is a very important clarification. In our opinion the transfer of data to a third country for reasons of public interest of that third country should not be allowed, i.e. we agree that the public interest must be recognised in Union law or in the national law of the Member State to which the controller is subject. In addition, we support the new provision introduced in the second sentence of this paragraph. Member States should be able to prohibit, in the public interest, data transfers.

PORTUGAL

Article 44 - Derogations

The proposed wording deserves agreement except in relation to sub-paragraphs d) and h) of paragraph 1.

In subparagraph d), we propose to replace the term "public interest" by "significant public interest". The regulation may, by way of example, indicate what is considered as "significant public interest".

With respect to subparagraph h), we propose to reformulate it or eliminate it. In fact, even an infrequent or a non massive transfer may involve a data transmission that would seriously damage the holder.

ROMANIA

General remark

Taking into account that Chapter V specifically regulates data transfer to third countries or international organizations, Romania considers necessary that the notion of data transfer should be defined within the text of the regulation in Art. 4, in order to ensure legal certainty regarding the rules of transfer. We propose the following definition:

"(20) 'transfer of personal data to third countries or international organizations' means a transmission of personal data, object of a processing or intended to be processed after the transfer, while the third country or international organization ensures an adequate level of protection which must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations, as provided in Chapter V of the present Regulation."

Bearing in mind the state of the art of digital technology, we have to acknowledge the significant importance of personal data transfer. There is need of more clarity about what data transfer means and implies, taking into account the fast development of cloud computing in recent years. Romania has often argued that this aspect has to be cautiously approached so as the principles of necessity and proportionality, be observed when performing a transfer. There needs to be more clarity established as to the safeguards in place when data is transferred to third countries.

Specific remarks

Art. 40

Romania agrees with the deletion of article 40 taking into account it's general stipulations, we consider it should be moved within a recital from the text of the regulation. We are of the opinion that the provisions of chapter V lack flexibility, they should give some more room for manoeuvre to the stakeholders.

Art. 41, paragraph 2

Romania supports the idea that the EDPB should be involved in the process of elaborating adequacy decisions.

Art. 41 paragraph 6

(...) A decision (...) pursuant to paragraph 5 (...) is without prejudice to transfers of personal data to the third country, or the territory or (...) processing sector within that third country, or the international organisation in question 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 giving rise to the Decision made pursuant to paragraph 5

At the same time, we consider that the phrase "at the appropriate time" needs to be clarified in order to be able to determine the exact date for beginning the consultations and the moment which the prohibition to transfer data to the third country/international organization becomes enforceable.

Art. 41 paragraph 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 in respect of which decisions have been taken pursuant to paragraphs 3 and 5.

RO welcomes a list with countries that provide an adequate level of protection, but does not welcome the list with countries that don't provide an adequate level of protection (blacklist). We consider that such list could cause possible political tenisons once it is published in the Official Journal; consequently, we propose the deletion.

Art. 42 paragraph 1

RO supports the insertion of the provisions regarding legally binding safeguards that should be ensured by the operator and processor in the absence of an adequacy decision by the Commission.

Art. 42 paragraph 5

"5. Where, nothwithstanding the requirement for a legally binding instrument in paragraph 1, the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor, being a public authority or body, shall obtain prior authorisation from the competent supervisory authority for any transfer, or category of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such a transfer. (...)."

Referring to paragraph 5, the intruments it refers to are not legally binding, that is why there is a risk of lowering the protection of personal data. The third country party is not bound by the administrative arrangement, so we are concerned how the appropritae safeguards will be ensured in such an instrument. An administrative arrangement is easier to be unilaterally denounced.

Furthermore, it is necessary to be established how this paragraph will be implemented in practice by the **public authorities.**

Art. 43 paragraph 3

[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.]

We propose that EDPB be envolved in the process of drafting and drawing up of the delegated and implementing acts that spcify the criteria laid down in paragraph 2, taking into account the broad expertize in the filed of its members and the advisory status of the EDPB.

Art. 43 paragraph 4

"4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers,...."

RO suggests the deletion of the wording "by electronic means" in order to ensure the technological neutrality of the regulation.

Art. 44 paragraph 1 letter d)

"(d) the transfer is necessary for important reasons of (...) public interest, this must be a public interest recognised in Union law or in the national law of the Member State to which the controller is subject ;

The reference to "**important reasons of public interest**" is too broad; there is a need to clarify at least what is meant by "public interest".

Art. 44 paragraph 1 letter g)

"[(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]"

RO would like that details and further clarifications regarding the scope of the provisions and the nature of the registers it refers to, be stipulated in a recital.

Art. 44 paragraph 1 letter h)

"(h) the transfer which is not large scale or frequent, is necessary for the purposes of legitimate interests pursued by the controller or the processor and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, where necessary, based on this assessment adduced suitable safeguards with respect to the protection of personal data;"

The criterion put forward in point h) is too vague and lacks legal clarity. Therefore, we propose that point (h) be removed.

Art. 44 paragraph 6

"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 (...)"

Taking into account that we propose the deletion of letter h), and in order to minimize the administrative burden of the controller and processor, especially in the public sector, we suggest to remove this paragraph.

Art. 45

RO requests to insert at this article a new pharagraf dealing which the issue of existing agreements.

Art. 66

(ca) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 38 and 39;

(cb) give the Commission an opinion on the level of protection in third countries or international organisations;

Reffering to paragraph 1, RO supports the extention of the EDPB competences regarding the issuing of opinions on the level of data protection in third countries or international organisations in cases of transfer.

SLOVAK REPUBLIC

Article 40

We consider as appropriate to define "third country" because it is not clear if this term relate to countries which are not members of the EU or to contracting parties of the agreement on European Economic Area.

The term "third country" used in Article 40 is not specified in Article 4 defining basic concepts of this Regulation proposal. We consider, for the reason of legal certainty, to specify and define this term in Article 4 of the Regulation proposal. Its definition will contribute to uniform interpretation of this term within all member states and will avoid its different interpretation when Regulation will be implemented in practice.

The detailed coverage of the matter of subsequent transfers of personal data should be amended to general principles. It is necessary to express normative principle to ensure that the possible transfer of data to country ensuring an adequate level of data protection would be protected in the case of subsequent transfer to country with inadequate level of data protection. In this context it is necessary take in mind possibilities of controller when using a cloud computing. We also believe that the basic approach to the issue of the data disclosure and its cross-border transfer should be solved in general principles of transfers. How to approach to data already disclosed onto an internet? Should not we supplement the conclusion wording of the judgment of the European Court of Justice in case of Bodil Lindquist (C-101/01) that "There is no transfer [of data] to a third country … where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country"? Considering the limited binding force of the European law, a reflection of the above conclusion could be considered directly in the Regulation proposal.

Other comments and suggestions to this Article that were raised by the delegations at the meetings, we insist on.

Article 41(1)

It is not clear for us or more precisely, we do not consider as a legally exact to use the term "processing sector" in wording of Article 41(1). In our opinion, this formulation of the provision in question seems to be redundant. We have the same reservation to Article 41(7).

Article 41(2)a

We consider as appropriate to supplement also assessment of the general protection level of fundamental human rights and freedoms forasmuch as a level of functioning of the legal state does not automatically mean an involvement in the international system of human right protection which is created by the framework of already agreed international and regional conventions on protection of fundamental human rights or membership in international organisations of human rights protection.

Other comments and suggestions to this Article that were raised by the delegations at the meetings, we insist on.

Article 42 - generally

The criterion for assessment of adequate level of data protection should be extended and linked to guarantees provided by Regulation proposal itself. The Slovak Republic identifies itself with proposed modification of the Article 42(1) of the Regulation proposal which is stated in the report of the European Parliament Committee LIBE.

Furthermore, we deem as appropriate to consider supplementing of legal provision providing the member states DPA with power to be allowed to impose a ban on controllers or processors to transfer the personal data to third countries as well as condition to impose such a ban.

The reason is to ensure a more efficient performance of supervision on secure processing of personal data which will reflect to up to date processing of personal data. The supervisory authority would be able to obtain further authorisation which will strengthen level of the personal data protection as well as reinforcement of data subject rights according to Chapter III of the Regulation proposal. The present supplement will contribute to the flexibility of the transfer restrictions when the Commission, based on the longer decision process, would not reflect to suddenly generated cases, whereby realisation of transfer itself could harm a data subject.

Other comments and suggestions to this Article that were raised by the delegations at the meetings, we insist on.

Article 42(1) and (2) together

Article 42(1) refers to Article 41 when the Commission has taken no decision the whole responsibility or adoption of security of data transfer to the third country or international organisation is imposed to controller or processor. It is necessary to closely specify term stated in Article 42(1) "legally binding instrument" as the controller or processor is able to take such a risk connected with their responsibility for transfer.

Generally we understand legally binding instrument as a legal provision/procedure according to law containing a certain level of legal power and which is binding for the same range of audiences and its enforcement is real. It must also be an instrument that will be or is already enshrined in the legal system of concerned country or international organisation.

It is necessary to specify this term for the application of this article and future application of the Regulation in practice. There is further necessary to clarify wording "… has adduced appropriate safeguards… in a legally binding instrument".

Article 43(3)

We support that the European Committee for Personal Data Protection will replace the Commission in respect to further specify closer criteria and requirements for binding corporate rules by delegated acts or at least to set out its participation in this task. The European Committee for Personal Data Protection represents by us such expert body that cannot be omitted when binding rules for regulation of binding corporate rules are created. We do not consider provision of the Article 87(2) as adequate assurance for participation of the Committee.

Other comments and suggestions to this article that were raised by the delegations at the meetings, we insist on.

Article 44(1)(h)

We consider as a necessary to define what we understand by the term "frequent or massive" in context of the cross-border transfer of personal data to the country with no adequate level of data protection. What point of view we will look at these concepts from; how it can be evaluated objectively, if something is frequent? One controller can have such legitimate interest once a year, other no once for five years and after this period he will have the "legitimate interest" three times. What criterion will be taken into account? How will be the time frequency and massive proved to – within the meaning of the whole lifetime of the operator, or in terms of the calendar year, or the percentage rate will be assessed on all transfers made by the operator and processor and some ceiling will be determined? That concept must be precise in terms of the answers to the above questions and to clear application and interpretation of the term for practical application of the Regulation.

Likewise, we consider as needed to clarify and redefine in context of the Article 44(6) *"…legitimate interests pursued by the controller or the processor…"*. It is possible to interpret the term *"legitimate interests of the controller or processor"* from different perspectives, e.g. it may be economic interests. It would be needed to closely specify this term or replace it by other notion, which would closely and better specify what interests must be in stake that the level of risk corresponds to these interests.

Other comments and suggestions to this Article that were raised by the delegations at the meetings, we insist on.

Chapter V

Art. 41

Towards paragraph 1 SK is of the opinion that the term "processing sector" is unclear and we consider it superfluous. We have a similar comment towards Art. 41(7) including other provisions where this term is used. We also maintain our comment in footnote 11.

Paragraph 3 in our opinion with regards to an established systematics of legal act it should be included in final provisions of the Chapter XI.

Art. 42

We would like to withdraw our scrutiny reservation in footnote 33 and express support to concept of cross-border data flows based on appropriate safeguards. However we have a strict reservation towards adding "recipient or recipients" into Paragraph 1 since it concerns subject with different legal position that controllers or processors. In our opinion it is necessary to apply the concept of legal regulation based on appropriate safeguards with regard to cross-border flows to third countries not ensuring appropriate level of data protection also on controllers and processors as importers of personal data.

Towards Paragraph 5b we have the same comment as towards Paragraph 3 of Art. 41 and we consider it more appropriate to include it in the Chapter XI.

Art. 43

SK in general supports highlighting significance of use of the BCR, therefore we would like to be included among delegations in the footnote 47.

In Paragraph 1 Point a) we would welcome further explanation of the term "group of undertakings or group of enterprises engaged in a joint economic activity". From the linguistic point of view in the course of translation into Slovak we have a problem distinguishing these two groups of businesses. We also support BE proposal in the footnote 49.

In Paraghraph 2 we strongly recommend maintaining construction of minimum demonstrative enumeration of content requirements of BCR in such a way that they shall generate their minimum standard which may be extended in individual cases according to the consideration and needs of group of undertakings. Therefore we ask for preservation of "at least" in the Paragraph 2. As for the specific content requirements enumerated in Paragraph 2 we welcome their specification but we would like to add Point h) which would state that the mandatory element of the BCR should be designation of main establishment for the group of undertakings.

Art. 44

SK in general welcomes specific legal grounds for cross-border flows for the sake of maintaining certain well-established continuity even against the realistic assumptions of some delegations that it may lead to setting aside of the BCR and standard contractual clauses in some cases. Our opinion is that the specific legal grounds for the cross-border flows should be used ad hoc and continuous flows should be governed by the BCR and standard contractual clauses.

We strongly welcome precision of Point d) with regard to needs of the public sector.
In Point e) we agree with PL that it needs further clarification since it is not clear whose legal claims should be defended, controller´s or data subject´s. It is also not clear if this provision concerns legal claims based on the Union, Member State´s or third country´s law.

Towards Paragraph 1 point h) we would welcome further clarification of "large scale" for the sake of legal certainty in a manner which shall stipulate that it concerns volume or quantity of data being transferred. Similarly we would welcome clarification of "frequent" which may currently be explained too subjectively.

In Paragraph 6 our opinion is that every transfer must be safeguarded by appropriate technical and organisational measures therefore it is not necessary to highlight a need to document the assessments well as suitable safeguards for one specific derogation or specific legal ground.

FINLAND

General remarks

A "third country" ***should be defined in article 4 as a country outside the European Union. Alternatively the words "third country" in Chapter V should be replaced by the words "country outside the European Union".***

It should also be clarified what is meant by an *"international organisation"* ***and with a*** *"transfer"* ***to a third country. It should be made clear whether/when mere loading of personal data on Internet constitutes a "transfer" of data to a third country.***

CHAPTER V

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

General remarks

The principles for transfers of personal data to third countries and international organisations are of utmost importance and therefore the articles in Chapter V have to be perfectly clear. The duties that the Regulation lays upon the controllers and processor in connection with these transfers must be unambiguous also in the context of cloud computing. It seems necessary to make an effort to specify the provisions in this respect.

Article 40

General principle for transfers

General remarks

The article states that "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…"

Following questions need to be answered:

1) What is meant by "intended" for processing? Also e.g. mere storage/retention and erasure of data is" processing" of data. Therefore we do not understand in which situations the data are only intended for processing after the transfer.

2) Intended for processing after transfer by whom and where? By the controller or the processor who transfers the data to be processed in a third country/in the cloud and then gets it back? Or by the recipient (controller or processor) in a third country or in an international organisation? Or by someone in the EU or in a third country to whom the above-mentioned recipient onwards the data?

At this stage, before getting further clarifications, and because personal data are always undergoing processing when they are transferred, we see that the wording " which are undergoing processing or are intended for processing after transfer" should be deleted.

We are not convinced that it is possible for the controller and processor to comply with the obligation in the last clause of the article. An onward transfer from a third country or an international organisation must in our view comply with that country´s law, not with EU law.

Any transfer of personal data (…) 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

Transfers with an adequacy decision

General remarks

We are in favour of adequacy decisions also in respect of a territory or a processing sector within a third country. We believe that these decisions would facilitate transfers of data to third countries without lowering the level of data protection.

We don´t see a need for decisions of lacking adequacy and therefore we think that paragraphs 5 and 6 should be deleted. So far the Commission has made no inadequacy decisions. Furthermore these decisions would be politically quite challenging to make. In case the possibility for the Commission to make decisions of lacking adequacy is kept in the Regulation, it is important that it is clear that in such cases transfers to the country in question will be possible on other grounds for transfers provided for in the Regulation.

Since the level of data protection in a third country may change, Commission´s decisions of adequacy should be regularly reviewed.

Everybody whose data are being transferred should have equally effective and enforceable rights. The last clause in paragraph 2 (a) should be amended accordingly.

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.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to 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 (…) whose personal data are being transferred;
(b) the existence and effective functioning of one or more independent (…) 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
(c) the international commitments the third country or international organisation in question has entered into.

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).

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.

5. (…)
6. (…)

5. 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 (…)ensured.

6. 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.

Article 42

Transfers by way of appropriate safeguards

General remarks:

It remains unclear to us when transfers to third countries could substantially affect the free movement of personal data within the Union as foreseen in paragraphs 4 and 5. Therefore we suggest deleting this wording from paragraphs 4 and 5 (from paragraph 6 in our suggestion).

Article 42 includes now both material and procedural provisions (e.g. the need for the supervisory authority to apply the consistency mechanism in paragraphs 4 and 5). We would prefer the material and procedural provisions to be clearly separated. This would make the text clearer and easier to read and understand.

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 (…) if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument or if the controller or the processor has obtained prior authorisation for the transfer by the supervisory authority in accordance with paragraph 5.

2. The legally binding instruments referred to in paragraph 1 are(…) in particular:
(a) binding corporate rules referred to in Article 43; or
(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
(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

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.

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 (…) from the 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 from the supervisory authority for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the legal basis for such transfer. (…)

6 (…)

7. (…)

8. 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.

Article 43

Transfers by way of binding corporate rules

General remarks

We support the aim to provide a legal basis for transfers by using "binding corporate rules".

According to the definition of "binding corporate rules" in article 3 (17) they mean "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 ore more third countries within a group of undertakings".

We think it might be useful to allow even a wider use of BCRs by allowing their use also in transfers between defined groups of enterprises that work very closely together in the same field (e.g. air carriers).

It would be useful to clarify in points (b) of paragraph 1 and (e) of paragraph 2 that the rights they refer to are rights that the data subjects have concerning processing of their data in a third country. The right to transfer data from EU by using BCR:s and the rights of the data subject in this respect are determined by EU law.

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, 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;
(b) expressly confer enforceable rights on data subjects in regard to the processing of their personal data in a third country on the bases of the binding corporate rules;
(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify:

(a) the structure and contact details of the group of undertakings and 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;

(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;

(e) the rights of data subjects in regard to the processing of their personal data in a third country on the bases of the binding corporate rules 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;

(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;

(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;

(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;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the policies 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.

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.

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).

Article 44

Derogations

General remarks

We think that the Commission should not be empowered to adopt delegated acts for the criteria and requirements for appropriate safeguards referred to in point (h) paragraph 1. Delegated acts seem unnecessary in view of paragraphs 3 and 6. Therefore paragraph 7 should be amended accordingly. Where the processing is based on point (h) paragraph 1, paragraph 3 provides for what the controller or processor shall give particular consideration to. According to paragraph 6 they also have to document the assessment as well as the appropriate safeguards and inform the supervisory authority of the transfer. We think that these safeguards are sufficient.

Even though point (g) paragraph 1 is practically identical with article 26.1 (f) in directive 95/46/EC, point (g) paragraph 1 needs to be clarified in the recitals by mentioning examples of the registers it refers to.

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:
(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
(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
(d) the transfer is necessary for important grounds of public interest; or
(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
(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
(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.

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.

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.

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.

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.

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. (…)

Article 45

International co-operation for the protection of personal data

General remarks

Article 45 paragraph 1 point (b) concerning mutual assistance is as it now stands unclear and far too general.

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;
(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;
(d) promote the exchange and documentation of personal data protection legislation and practice.

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).

SWEDEN

Introduction

The Presidency has invited delegations to send in proposals for amendments or comments regarding Chapter V of the General Data Protection Regulation. Sweden welcomes the Presidency's initiative and presents in this paper some comments and proposals for amendments, in addition to those already put forward at the meetings of the working party.

We would like to underline that the comments and proposals are preliminary and that we maintain a general scrutiny reservation and a reservation regarding the legal form of the instrument. We may provide new comments and suggestions when the working party revisits these articles.

~~**Bold strikethrough**~~ indicates proposed deletions.

[Bold in brackets] indicates provisions that need further consideration.

Article 40

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.]

Comment: We are not convinced of the need for this article. By way of general comment, it should be considered to include a definition of transfer in the regulation, e.g. to make it clear that publication on the internet is not considered a transfer.

Article 42

Transfers by way of appropriate safeguards

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.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

   (a) binding corporate rules in accordance with Article 43; or

   (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

   (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

   (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

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.

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.

Comment: Deleted in consequence to the suggested deletion of paragraph 6 (former Article 34(1).

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.

Comment: Deleted in consequence to the suggested deletion of paragraph 6 (former Article 34(1).

~~6 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 mitigate the risks involved for the data subjects where a controller [or processor] adopts contractual clauses as provided for in point (d) of paragraph (2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in paragraph (5) for the transfer of personal data to a third country or an international organisation.~~

Comment: This paragraph adds little or no value compared to paragraphs 4 and 5 and could be deleted.

Article 44

Derogations

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:

(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

(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

(d) the transfer is necessary for important grounds of public interest; or

(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

(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

(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.

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.

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.

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.

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.~~**

Comment: The obligation to inform the supervisory authority appears to be an disproportionate administrative burden.

~~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.~~

UNITED KINGDOM

General Comments

We welcome the opportunity, provided by the Presidency of the Council, to make written comments and observations on Chapter V of the proposed Regulation. At this stage, we would want to place a general scrutiny reserve on this chapter, so we can consider the package as a whole before reaching a definitive view on these provisions.

However, as a starting point, we think the system of international data transfers needs a complete rethink. We consider that it contains three significant flaws: it is outdated, unbalanced (in the sense that the hugely burdensome requirements can in fact by bypassed) and unfit for modern processing.

In terms of the model being outdated, this system (in which transfers are subject to a heavily bureaucratic processes to authorise them) dates back to the 1970s. It is neither realistic nor practical to continue with it.

The system is unbalanced and lacks credibility. It imposes a very costly and bureaucratic system for data transfers, but allows controllers to go round this system by relying on the derogations in Article 44.

It is an unavoidable reality that data is already in free flow across the globe, crossing borders at the click of a button. It is neither practical nor possible to stem this flow, neither should we attempt to do so, because of the risk to technological development and harm to economic growth.

For these reasons the development of a new model essential to making the instrument credible and relevant for processing now and in the future.

Further general observations

Bearing in mind the frequency with which data moves in and out of the EEA, it may be that there is no point in distinguishing between international data transfers and transfers within the EEA: the fact that data is transferred outside the EEA could be a factor which the controller should take into account in the course of assessing the risk of processing, for example when considering matters such as data security and conducting risk assessments. In other words international transfers would be woven into the substantive provisions, rather than being a separate aspect of data protection. Innocuous data could possibly be transferred with few if any supplementary safeguards beyond those already provided for in other Articles. We will consider these issues further.

There is also a fundamental question about whether the concept of a transfer is still valid. Data can be accessed from outside the EEA without the controller transferring it, and copied or downloaded by an individual located outside the EEA. This lacuna is not addressed in the current draft of Chapter V.

The obligations under Chapter V are over and above the substantive obligations in the Regulation. Where a data controller is transferring data abroad, the transfer itself will constitute processing under the Regulation, so the requirements under Chapter V will apply in addition to the other obligations. Any further obligations will need to be precise, proportionate and necessary in the particular case.

Article 40

We agree with those Member States who took the view that Article 40 is superfluous.

Article 41

General points

We agree with the Presidency that a risk-based approach is important for data protection. We don't think adequacy fits into the risk based model because it takes no account of the context of a particular transfer and crucially the data being processed. Therefore whilst we have no wish to repeal adequacy decisions already taken, we don't see that there is a place for new findings of adequacy under the Regulation.

The concept of adequacy is unclear. It appears not to mean that the data protection standards in the relevant country or sector need to be the same as in the EU, but it is far from certain what test the relevant sector or country must meet in order to be deemed adequate. This is not satisfactory.

Detailed comments

Paragraph 2

We consider that there are problems with the list set out here. We don't think that the Commission is in a position to analyse matters such as national security in another country, which is a field outside its area of expertise and competence.

The translation and interpretation of a third country's legislation and international commitments does not seem to be a good use of the Commission's time or of European taxpayers' money. Further, adequacy is too blunt an instrument to deal with the consequences of individual transfers which pose a high degree of risk to data subjects. It is not at all clear that having an adequate standard of protection in the third country to which the data will be transferred actually provides sufficient safeguards for the data subject in a given situation.

Paragraphs 5 and 6

The idea of deciding that a transfer to a particular third country should be prohibited could have a significant destabilising effect on diplomatic relations. We therefore consider that paragraphs 5 and 6 are unworkable. Further, it seems illogical that the lack of adequacy doesn't in fact preclude transfer to that country in any event under Articles 42 to 44.

Article 42

Article 44 contains the core of Chapter V. We think it sets out circumstances in which data should be able to be transferred outside the EEA as a rule, rather than on an exceptional basis. Such a transfer may be effected pursuant to a contract under Article 44(1)(b) or under an MOU under paragraph 1(d). However, we don't consider that further safeguards as set out at Article 42(2) would be necessary in most cases, bearing in mind that the controller is already subject to the substantive requirements in the Regulation and is liable for any processing under it in any event (see Article 5(f)).

Article 42 as it stands creates significant risks of paralysing data transfers outside the EEA. This will be a particular problem at the point when the Regulation comes into force. Under the '95 Directive controllers could make their own assessment of adequacy, but this is no longer the case under the Regulation. Therefore many more controllers may be looking to supervisory authorities to authorise transfers, for example under paragraph 2(d) and 4. Further, the requirement at paragraphs 4 and 5 that the consistency mechanism is applied in processing activities concerning data subjects in more than one member state risks creating further prolonged periods of uncertainty. Of course the answer for many controllers may simply be to rely on the derogations in any event, thus circumventing Article 42.

Article 43

As set out above in relation to Article 42, we consider that the core of Chapter V is in Article 44. If the emphasis of Chapter V is changed to reflect this, then Article 43 will need to be reconsidered.

If the proposal is to remain as it is then it is likely that supervisory authorities will be inundated with requests for approval of BCRs. The bottlenecks which will inevitably result from this system are likely to have a detrimental impact on day to day business operations and businesses will be increasingly likely to rely on derogations under Article 44 to effect transfers.

Article 44

General comments

The derogations in this Article can be grouped into three categories: where the risks to the data subject are relatively small; where the other public interests override the data subject's rights; where the transfer benefits the data subject. This being the case, we think that the classification of these categories as derogations is wrong. In all three categories the processing is both necessary and justifiable. Transfer of data falling into these categories should therefore be the rule rather than the exception.

Detailed comments

There seems to us to be no justification for limiting transfers under paragraph 1(h) to those which are not "frequent or massive". If the transfer is necessary for legitimate interests pursued by the controller and where those interests do not override the interests or fundamental rights and freedoms of data subjects then there is no reason why the transfer should not go ahead, even where it is "frequent or massive".

As we have stated elsewhere, we consider that public authorities should be entitled to rely on legitimate interests as a ground of processing.

Article 45 – International co-operation for the protection of personal data

We question the need for Article 45 of the system of adequacy is to be dispensed with. The international role of supervisory authorities could be dealt with in Chapter VI.

SUISSE

Switzerland thanks the Presidency for the opportunity to comment on chapters V-VII of the proposal for a General Data Protection Regulation. A differentiation between provisions for the public sector and provisions for the private sector in these chapters is of our major concern.

Therefore we would welcome solutions which take into account the specifics of processing of personal data by public authorities. In our view – and as an example - Article 42 paragraph 4 should not be applicable for data processing by public authorities. A transfer of personal data by public authorities to a third country should not be subject to prior authorization from the supervisory authority. Article 58 paragraph 2 is of a similar kind. In our understanding any measure according to Article 58 paragraph 2 is limited to data processing by private actors. This fact should be pointed out more explicitly in the text of the Regulation.

NORWAY

Norway is in favour of a practicable and efficient system regarding adequacy decisions. In Chapter V on transfers of data, the Commission is to make decisions on adequacy. Considering especially the high number of adequacy decisions that need to be taken, we believe that the current system where adequacy can be decided at national level should be considered as an alternative.

Furthermore we are concerned that the Member States' possibility to report to international organizations and third countries in order to fulfil obligations in international agreements might be rendered difficult under the proposed draft. A legal basis for such reporting could be ensured through the inclusion of a derogation covering such cases in Article 44.