**COUNCIL OF THE EUROPEAN UNION**

**Brussels, 28 May 2014**

**10349/14**

**Interinstitutional File: 2012/0011 (COD)**

**DATAPROTECT 85**
**JAI 375**
**MI 467**
**DRS 74**
**DAPIX 73**
**FREMP 106**
**COMIX 292**
**CODEC 1384**

**NOTE**

| | |
|---|---|
| from: | Presidency |
| to: | Council |
| No. prev. doc.: | 9865/2/14 REV 2 DATAPROTECT 71 JAI 312 MI 425 DRS 68 DAPIX 64 FREMP 90 COMIX 263 CODEC 1294 |
| 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)<br>– Partial General Approach on Chapter V |

**Background**

1. Transborder information flows are an inherent element of today's globalised and interconnected world, which requires the adaptation of the regulation to keep pace with these developments and to ensure the continuity of the high protection offered to individuals in the EU both when they are targeted by companies established outside the EU and where their personal data are being transferred to third countries or international organisations. During the January 2014 informal discussions of Athens and during the JHA March 2014 Council Ministers discussed issues relating the international dimension of the data protection reform.

During the January 2014 informal discussions of Athens, Ministers expressed their overall satisfaction with the provisions of the draft regulation on international transfers and with the territorial scope of the Regulation, highlighting the need to broadly ensure the application of Union rules to controllers not established in the EU when processing personal data of Union residents.

2. During the March Council, the draft provisions as regards the territorial scope of the regulation as defined in Article 3(2) were broadly supported, highlighting the need to broadly ensure the application of Union rules to controllers not established in the EU when processing personal data of Union data subjects. Ministers also confirmed their understanding that international transfers of personal data to third countries should take place on the basis of the structure and the key principles contained in Chapter V. They also underscored the exceptional nature of the transmission of personal data to third countries or international organisations based on derogations (i.e. when not based on findings of adequacy/appropriate safeguards including binding corporate rules or contractual clauses) and the need to provide safeguards to ensure the fundamental rights and freedoms as regards the protection of personal data as enshrined in Article 8 of the EU Charter. Ministers agreed that more technical work needed to be done on Chapter V, including the discussion on possible alternative/supplementary models for international data transfers.

3. The General Data Protection Regulation builds on the proven system and principles of the Data Protection Directive (Directive 95/46/EC). It provides a framework for transfers, which relies on adequacy decisions, appropriate safeguards and, in absence of them, on derogations for specific situations as laid down in the Regulation.

4. The draft Regulation carries forward the approach of transfers with an adequacy decision, where the Commission may decide, in the framework of comitology, with the involvement of Member States representatives and scrutiny of the European Parliament, whether the level of protection ensured by a third country – including certain territories or specified sectors, such as specific economic sectors - or an international organisation is adequate. The compromise text provides that the European Data Protection Board shall give the Commission an opinion both for the assessment of the adequacy of the level of protection in a third country or international organisation and for the assessment whether the third country or international organisation or the specified sector no longer ensures an adequate level of protection. Further specifications have been made with respect to the elements to be taken into account when deciding on the level of adequacy (including an explicit reference to third country's accession to the Council of Europe Convention 108[1]) and regarding the duty of the Commission to monitor the functioning of adequacy decisions within a reasonable period.

5. The compromise text provides explicitly that transfers to third countries can take place if the data controller or the processor applies appropriate safeguards, including by way of approved codes of conduct or an approved certification mechanism which is currently not foreseen. Furthermore, a classification is operated between appropriate safeguards, which do not require any specific authorisation from supervisory authorities (i.e. BCR's, standard data protection clauses as well as approved codes of conduct and certification mechanisms ensuring the commitment of the controller, processor or recipient in the third country to guarantee the protection of the personal data originating from the EU) and appropriate safeguards that remain subject to authorisation from the competent supervisory authority (in particular contractual clauses not based on agreed standard contractual clauses).

[1] Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol.

6. Transfers can also be based on derogations in specific situations. Further clarifications have been made about the criteria to be taken into account and on the important reasons of public interests (e.g. between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health or for reduction and elimination of doping in sport).

7. Furthermore, some Member States requested the introduction in the draft Regulation of an explicit provision authorising the limitation of transfers to third countries in cases of important reasons of public interests. The Presidency has introduced a provision (Article 44, 5a) allowing such limitations in the absence of a Commission adequacy finding, with a notification of the national measures to the Commission.

8. As regards possible future new models (alternative/supplementary ) that could be envisaged for international transfers, no such models have been proposed by Member States. The Presidency considers that these can and should inscribe themselves in the logic of the – multifaceted but yet coherent – system currently proposed for which Ministers have given their support. The current compromise is future-proof and provides sufficient possibilities to accommodate new models based on appropriate safeguards ensuring the protection of individuals whose data are transferred abroad.

9. At the DAPIX meetings of 31 March -1 April, 7 May and 15-16 May 2014, the text of Chapter V was further discussed in order to finalise the remaining issues. Following the discussions at COREPER on 28 May 2014, the Presidency has further revised the text and the corresponding recitals. The latest changes are indicated in **bold underlining**.

**Partial general approach**

10. The Presidency invites the Council to reach a partial general approach on Article 3(2) (territorial scope), on the respective definitions of BCR and "international organisation" (Articles 4 (17) and (21)) and on Chapter V contained in the Annex on the following understanding:

    i. such partial general approach is to be reached on the understanding that nothing is agreed until everything is agreed and does not exclude future changes to be made to the text of Chapter V to ensure the overall coherence of the Regulation.

    ii. such partial general approach is without prejudice to horizontal questions, such as the legal nature of the instrument or provisions on delegated acts

    iii. such partial general approach does not mandate the Presidency to engage in informal trilogues with the European Parliament on the text.

11. With a view to reaching this partial general approach the following three issues have received particular attention:

*Need to obtain prior authorisation in case of appropriate safeguards (Art 42)*

12. The compromise text distinguishes:

    a) transfer without specific authorisation in case of legally binding instruments; and

    b) transfer requiring authorisation by the competent data protection authority in other cases.

The new text clarifies that these approved codes of conduct and certification mechanisms must go together with a binding and enforceable commitment from the controller or processor in the third country. In the future, this will also need to be reflected in the wording of the corresponding articles (38- 39) in Chapter IV[2].

[2] Thus it could be envisaged that Article 39 would allow for a European-wide certification scheme in such cases and would list the European principles to which the controllers or processors in third countries should comply with, and the appropriate safeguards that they should implement to obtain such certification. A list of certified controllers or processors could be published and regularly updated under the responsibility of EDPB.

*Transfers for a legitimate interest of the controller (Art 44 (1h))*

13. Beyond transfers on the basis of an adequacy finding issued by the Commission or appropriate safeguards (BCRs, contractual clauses, codes of conduct etc.), which are applicable to public and private sectors including NGOs, transfers can be based on the derogations listed in Article 44. One of these derogations, set out in Article 44(1)(h), allows a transfer for legitimate interests pursued by the controller under the condition that:
    - the transfer may not be large scale or frequent, that is it has an occasional/character; and
    - the legitimate interests of the controller may not be overridden by the rights and freedoms of the individual concerned ( =data subject); and
    - the controller adduces suitable safeguards, as explained further in recital 88.

14. The Presidency is of the opinion that the right balance has been struck and therefore this derogation should remain as currently drafted.

*Limiting the transfer of personal data to third countries (44 (5a))*

15. There may be an exceptional need for public authorities, for important reasons of public interest, to set limits to the flow of personal data outside the European Union, on the basis of Union or Member State law. One delegation has provided the example of national passport data and of electronic patient files[3]. This derogation, as now worded, appears to be acceptable to the majority of delegations.

---

[3] 9703/14 DATAPROTECT 68 JAI 303 MI 417 DRS 64 DAPIX 62 FREMP 88 COMIX 254 CODEC 1247.

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

20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment or not, which takes place in the Union. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging doing business with data subjects residing in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users residing in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union.

21) The processing of personal data of data subjects residing in the Union by a controller not established in the Union should also be subject to this Regulation when it is related to the monitoring of their behaviour taking place within the European Union. In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or[4] another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

[4] DE scrutiny reservation, querying especially about the application of the rules of place of purchase in relation to Article 89a.

79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of EU law and include safeguards to protect the rights of the data subjects[5].

80) The Commission may (…) decide with effect for the entire Union that certain third countries, or a territory or a specified sector, such as the private sector or one or more specific economic sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations, which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of a third country or of a territory or of a specified sector within a third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision to a territory or a specified sector in a third country should take into account clear and objective criteria , such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country.

[5] FR requests the second sentence to be inserted in Article 89a. NL asked what was meant with the new text and considered that it was necessary to keep it, but its purpose and meaning should be clarified. DE and UK scrutiny reservation on the new text. EE asked whether if "*affect"* means that it was not contradictory or something else.

81a) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol *should be taken into account*. The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations[6].

81b) The Commission should monitor the functioning of decisions on the level of protection in a third country or a territory or specified sector within a third country, or an international organisation, including decisions adopted on the basis of Article 25(6) or Article 26 (4) of Directive 95/46/EC. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any pertinent findings to the Committee within the meaning of Regulation (EU) No 182/2011 as established under this Regulation.

82) The Commission may (…) recognise that a third country, or a territory or a specified sector within a third country, or an international organisation (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

---

**6** DE, supported by NL, proposed 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). According to the position of DE, 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.

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or ad hoc contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. They should relate in particular to compliance with the general principles relating to personal data processing, the availability of enforceable data subject's rights and of effective legal remedies and the principles of data protection by design and by default. Transfers may be carried out also by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding. The authorisation of the competent supervisory authority should be obtained when the safeguards are adduced in non legally binding administrative arrangements.

84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract, including in a contract between the processor and another processor, nor to add other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

85) A corporate group or a group of enterprises engaged in a joint economic activity should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings or group of enterprises, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his explicit consent, where the transfer is occasional **(…)** in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

87) These rules should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange, between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, for example in case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent.[7] In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organization. Member States should notify such provisions to the Commission.

[7] FR referred to the situation of a recipient of the transfer who is a medical professional or has adduced provisions ensuring the respect of the data subject's right to privacy and medical confidentiality. PRES considers that this could be further addressed in the context of chapter IX.

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. The controller or processor should give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced suitable safeguards to protect fundamental rights and freedoms of natural persons with respect to processing of their personal data. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. (…)

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

107) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

*Article 3*

***Territorial scope***

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union[8].

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

[8] UK reservation.

***Article 4***

*Definitions*

For the purposes of this Regulation:

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings[9] or group of enterprises engaged in a joint economic activity;

(21) 'international organisation' means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries[10];

[9] DE queried whether BCRs could also cover intra-EU data transfers. COM indicated that there was no need for BCRs in the case of intra-EU transfers, but that controllers were free to apply BCRs also in those cases.

[10] NL queried whether MOUs would also be covered by this definition; FI queried whether Interpol would be covered. CZ, DK, LV, SI, SE and UK pleaded in favour of its deletion.

# CHAPTER V
# TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS[11] [12] [13] [14]

*Article 40*

***General principle for transfers***

(…)

[11] In light of the fact that the public interest exception would in many cases be the main ground warranting an international transfer of personal data, some delegations (CZ, DE, LV, UK) queried whether the 'old' adequacy principle/test should still maintained and set out in such detail, as it would in practice not be applied in that many cases. DE in particular thought that the manifold exceptions emptied the adequacy rule of its meaning. Whilst they did not disagree with the goal of providing protection against transfer of personal data to third countries, it doubted whether the adequacy principle was the right procedure therefore, in view of the many practical and political difficulties (the latter especially regarding the risk of a negative adequacy decision, cf. DE, FR, UK). The feasibility of maintaining an adequacy-test was also questioned with reference to the massive flows of personal data in in the context of cloud computing: BG, DE, FR, IT, NL, SK and UK. FR and DE asked whether a transfer of data in the context of cloud computing or the disclosure of personal data on the internet constitutes an international transfer of data. DE also thought that the Regulation should create a legal framework for 'Safe Harbor-like' arrangements under which certain guarantees to which companies in a third country have subscribed on a voluntary basis are monitored by the public authorities of that country. The applicability to the public sector of the rules set out in this Chapter was questioned (EE), as well as the delimitation to the scope of proposed Directive (FR). The impact of this Chapter on existing Member State agreements was raised by several delegations (FR, PL).

[12] NL and UK pointed out that under the 1995 Data Protection Directive the controller who wants to transfer data is the first one to assess whether this possible in under the applicable (EU) law and they would like to maintain this basic principle, which appears to have disappeared in the Commission proposal.

[13] DE asked which law would apply to data transferred controllers established in third countries that come within the ambit of Article 3(2); namely whether this would be EU law in accordance with that provision.

[14] AT has made a number of proposals regarding this chapter set out in 10198/14 DATAPROTECT 82 JAI 363 MI 458 DRS 73 DAPIX 71 FREMP 103 COMIX 281 CODEC 1351.

*Article 41*

***Transfers with an adequacy decision***[15]

1. A transfer of personal data to a third country or an international organisation may take place where the Commission[16] has decided that the third country, or a territory or one ore more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

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

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…)[17], both general and sectoral, data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that third country or international organisation, as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred (…)[18];

---

15 Some delegations raised concerns on the time taken up by adequacy procedures and stressed the need to speed up this process. COM stated that this should not be at the expense of the quality of the process of adequacy.

16 CZ, DE and SI reservation on giving such power to the Commission. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data. UK had considerable doubts on the feasibility of the list in paragraph 2.

17 AT would have preferred including a reference to national security.

18 NL thought that Article 41 was based on fundamental rights and legislation whereas Safe harbour is of a voluntary basis and that it was therefore useful to set out elements of Safe Harbour in a separate Article. DE asked how Safe Harbour could be set out in Chapter V.

(b) the existence and effective functioning of one or more independent supervisory authorities[19] in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules including adequate sanctioning powers for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States;

(c) the international commitments the third country or international organisation concerned has entered into, or other (…) obligations arising from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

2a. The European Data Protection Board shall give the Commission an opinion[20] for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.

[19] NL queried how strict this independence would need to be assessed. BE suggested adding a reference to independent judicial authorities, FI suggested to refer to 'authorities' *tout court*.

[20] CZ would prefer stronger language on the COM obligation to request an opinion from the EDPB.

3. The Commission, after assessing the adequacy[21] of the level of protection, may decide that a third country, or a territory or one or more specified sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. (…)[22]. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the (independent) supervisory authority(ies) mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2)[23].

3a. *Decisions adopted by the Commission on the basis of Article 25(6)* (…) *of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission*[24] in accordance with the examination procedure referred to in Article 87(2)[25].

---

[21] CZ, RO and SI reservation on giving such power to the Commission. DE thought that stakeholders should be involved in this process. NL and UK indicated that on this point the proposal seemed to indicate a shift from the 1995 Data Protection Directive, which put the responsibility for assessing a third country's data protection legislation in the first place with the controller who wanted to transfer personal data.

[22] CZ, DE DK, HR, IT, NL, PL, SK and RO thought an important role should be given to the EDPB in assessing these elements.COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.

[23] DE queried the follow-up to such decisions and warned against the danger that third countries benefiting from an adequacy decision might not continue to offer the same level of data protection. COM indicated there was monitoring of third countries for which an adequacy decision was taken.

[24] Moved from paragraph 8. CZ and AT thought an absolute maximum time period should be set (sunset clause), to which COM was opposed. NL, PT and SI thought this paragraph 3a was superfluous or at least unclear. Also RO thought that, if maintained, it should be moved to the end of the Regulation.

[25] DE and ES suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011. DE asked if a decision in paragraph 3a lasted forever. IE considered paragraph 3a providing necessary flexibility. CZ thought that new States should not be disadvantaged compared to those having received an adequacy decision under Directive 1995.

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC[26].

5. The Commission may decide that a third country, or a territory or a specified sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3)[27].

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

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or specified sector within that third country, or the international organisation in question pursuant to Articles 42 to 44[28].

---

**26** BE queried about the reference to the 1995 Directive. CZ perceives this as superfluous.

**27** FR and UK suggested the EDPB give an opinion before COM decided to withdraw an adequacy decision.

**28** DE asked for the deletion of paragraph 6. DK thought the moment when third countries should be consulted was unclear.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and specified sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3, 3a and 5.

8. (…)

*Article 42*

***Transfers by way of appropriate safeguards***[29]

1. In the absence of a decision pursuant to paragraph 3 of Article 41, a controller or processor may transfer personal data to (…) a third country or an international organisation only if the controller or processor has adduced appropriate safeguards, also covering onward transfers (…) .

[29] UK expressed concerns regarding the length of authorisation procedures and the burdens these would put on DPA resources. The use of these procedures regarding data flows in the context of cloud computing was also questioned.

2. The appropriate safeguards referred to in paragraph 1 *may* be provided for (…), without requiring any specific authorisation from a supervisory authority, by:

(oa) a legally binding **and enforceable** instrument **between public authorities or bodies**[30]; or

(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)[31]; or

(c) standard data protection clauses adopted by a supervisory authority and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2).

(d) an approved code of conduct pursuant to Article 38 together with binding and enforceable commitments of the controller or processor (…) in the third country to apply the appropriate safeguards, **including as regards data subjects' rights** ; or

(e) an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor (…) in the third country to apply the appropriate safeguards, **including as regards data subjects' rights**.

---

**30** HU has serious concerns; the proposed general clause ("a legally binding instrument") is too vague because the text does not define its content. Furthermore, the text does not provide for previous examination by the DPA either. HU therefore suggests either deleting this point or subjecting such instrument to the authorisation of the DPA, as it believes that there is a real risk that transfers based on such a vague instrument might seriously undermine the rights of the data subjects.

**31** FR reservation on the possibility for COM to adopt such standard clauses.

2a. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the data (…) in the third country or international organisation; or

(b) (…)

(c) (…)

(d) provisions to be inserted into administrative arrangements between public authorities or bodies (…).

3. (….)

4. (….)

5a. The supervisory authority shall apply the consistency mechanism in the cases referred to in points (ca), (d), (e) and (f) of Article 57 (2).

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority*[32]*. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission*[33] in accordance with the examination procedure referred to in Article 87(2)[34].

*Article 43*

***Binding corporate rules***[35]

1. The competent supervisory authority shall *approve*[36] *binding corporate rules* in accordance with the consistency mechanism set out in Article 57 provided that they:

(a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity;

---

32 UK and ES disagreed with the principle of subjecting non-standardised contracts to prior authorisation by DPAs. IT was thought that this was contrary to the principle of accountability. DE emphasised the need of monitoring.

33 AT thought an absolute time period should be set.

34 DE and ES have suggested to request the Board for an opinion. COM has pointed out that there can be no additional step in the Comitology procedure, in order to be in line with the Treaties and Regulation 182/2011.

35 NL thought it should be given a wider scope. BE and NL pointed to the need for a transitional regime allowing to 'grandfather' existing BCRs. NL asked whether the BCRs should also be binding upon employees. SI thought BCRs should also be possible with regard to some public authorities, but COM stated that it failed to see any cases in the public sector where BCRs could be applied. HU said that it thought that BCRs were used not only by profit-seeking companies but also by international bodies and NGOs.

36 DE and UK expressed concerns on the lengthiness and cost of such approval procedures. The question was raised which DPAs should be involved in the approval of such BCRs in the consistency mechanism.

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;

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

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the *concerned* group and of each of its members;

(b) the data transfers or categories of transfers, including the types of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

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

(d) application of the general data protection principles, in particular purpose limitation, (…) data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to (…) 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 concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage[37];

[37] DE thought that the reference to exemptions should be deleted here.

(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 Articles 14 and 14a;

(h) the tasks of any data protection officer designated in accordance with Article 35 or any other person or entity in charge of the monitoring (…) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

(hh) the complaint procedures;

(i) the mechanisms within the group, for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point h) and to the board of the controlling undertaking or of the group of enterprises, and should be available upon request to the competent supervisory authority;

(j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph[38];

(l) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules[39]; and

[38] BE suggested making this more explicit in case of a conflict between the 'local' legislation applicable to a member of the group and the BCR.

[39] CZ expressed concerns about the purpose of this provision and its application. UK found this point very prescriptive and wanted BCRs to be flexible to be able to be used for different circumstances.

(m) the appropriate data protection training to personnel having permanent or regular access to personal data (...).

2a. The European Data Protection Board shall advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules.

[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.][40]

4. The Commission may specify the format and procedures for the exchange of information (…) between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

[40] CZ, IT, SE and NL reservation. FR scrutiny reservation regarding (public) archives. RO and HR thought the EDPB should be involved. PL and COM wanted to keep paragraph 3.

*Article 44*

***Derogations for specific situations***[41]

1. In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, a transfer or a category 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 explicitly[42] consented to the proposed transfer, after having been informed that such transfers may involve *risks* for the data subject due to the absence of an adequacy decision and appropriate safeguards; or

   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

   (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 reasons of public interest[43]; or

   (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

---

41 EE reservation. NL parliamentary reservation. CZ, EE and UK and other delegations that in reality these 'derogations' would become the main basis for international data transfers and this should be acknowledged as such by the text of the Regulation.

42 UK thought the question of the nature of the consent needed to be discussed in a horizontal manner.

43 DE remarked that the effects of (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. IT reservation on the (subjective) use of the concept of public interest. HR suggested adding 'which is not overridden by the legal interest of the data subject'.

(f) the transfer is necessary in order to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer, *which* is not large scale or *frequent*[44], is necessary for the purposes of legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject and where the controller (…) has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and (…) based on this assessment adduced suitable safeguards[45] with respect to the protection of personal data.

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.

---

[44] AT, ES, HU, MT, PL, PT and SI would prefer to have this derogation deleted as they think it is too wide; it was stated that data transfers based on the legitimate interest of the data controller and directed into third countries that do not provide for an adequate level of protection with regard to the right of the data subjects would entail a serious risk of lowering the level of protection the EU acquis currently provides for.) DE and ES scrutiny reservation on the terms 'frequent or massive'. DE, supported by SI, proposed to narrow it by referring to 'overwhelming legitimate interest'. ES proposed to replace it by 'are small-scale and occasional'; UK asked why it was needed to add another qualifier to the legitimate interest of the transfer and thought that such narrowing down of this derogation was against the risk-based approach.

[45] AT and NL reservation: it was unclear how this reference to appropriate safeguards relates to appropriate safeguards in Article 42.

3. (…)

4. Points (a), (b), (c) and (h) of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers[46].

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.

5a. In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation[47]. Member States shall notify such provisions to the Commission[48].

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 (…).

6a. (…)

7. (…)

[46] BE scrutiny reservation. FR has a reservation concerning the exception of public authorities.

[47] SI and UK scrutiny reservation. FR and ES proposed that this provision should be included in another provision.

[48] Some delegations (FR, PL, SI) referred to the proposal made by DE (for new Article 42a: 12884/13 DATAPROTECT 117 JAI 689 MI 692 DRS 149 DAPIX 103 FREMP 116 COMIX 473 CODEC 186) and the amendment voted by the European Parliament (Article 43a), which will imply discussions at a later stage.

***Article 45***

*International co-operation for the protection of personal data*[49]

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

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

   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms[50];

   (c) engage relevant stakeholders in discussion and activities aimed at promoting 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. (…)

---

[49] PL thought (part of) Article 45 could be inserted into the preamble. NL, RO and UK also doubted the need for this article in relation to adequacy and thought that any other international co-operation between DPAs should be dealt with in Chapter VI. NL thought this article could be deleted. ES has made an alternative proposal, set out in 6723/6/13 REV 6 DATAPROTECT 20 JAI 130 MI 131 DRS 34 DAPIX 30 FREMP 15 COMIX 111 CODEC 394.

[50] AT and FI thought this subparagraph was unclear and required clarification.