



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 3 June 2013**

**9967/13**

---

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

---

**LIMITE**

**DATAPROTECT 67  
JAI 418  
MI 436  
DRS 103  
DAPIX 85  
FREMP 69  
COMIX 330  
CODEC 1175**

**NOTE**

---

from: Presidency

to: Working Group on Information Exchange and Data Protection (DAPIX)

---

No. prev. doc.: 6723/4/13 REV 4 DATAPROTECT 20 JAI 130 MI 131 DRS 34 DAPIX 30  
FREMP 15 COMIX 111 CODEC 394

No Cion prop.: 5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12  
FREMP 7 COMIX 61 CODEC 219

---

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)  
- Revised Chapter V

---

Further to the discussions in DAPIX and the written comments received, delegations find attached a revised version of Chapter V.

- (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 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 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.
- (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.
- (80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.
- (81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including public order and criminal law.

- (82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation (...) 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 and 43 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.
- (83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those 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.
- (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 consent, where the transfer is necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register 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 derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters or for public health, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent.
- (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. 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. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.
- (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.

# CHAPTER V

## TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS<sup>1</sup>

*Article 40*

*General principle for transfers*

(...)<sup>2</sup>.

---

<sup>1</sup> FR reservation. 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, CZ, LV, UK) queried whether the 'old' adequacy principle/test should still be 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 the context of cloud computing: BG, DE, FR, IT, NL, SK and UK. 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 (EE, FR, PL). FR requested that a grandfather clause be inserted preserving international agreements concluded by Member States.

<sup>2</sup> The Presidency agrees with GR, SE, NL and UK that this article has no added value to the rest of the Chapter V and has therefore deleted it., BE, supported by FI and NL, thought that the requirements regarding onward transfer need not be mentioned here, as these were at any rate subsumed under the adequacy requirement. FR thought the requirement of prior originator consent to onward transfer should be expressed in a different manner. ES was opposed to putting the processor and controller on the same footing.

Article 41

***Transfers with an adequacy decision***<sup>3</sup>

1. A transfer of personal data to a recipient or recipients in a third country or an international organisation may take place where the Commission<sup>4</sup> has decided that the third country, or a territory or a processing sector<sup>5</sup> within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific<sup>6</sup> authorisation.
2. When assessing the adequacy of the level of protection, the Commission<sup>7</sup> shall, in particular, take account of<sup>9</sup> the following elements:
  - (a) the rule of law, respect for human rights<sup>10</sup> and fundamental freedoms, relevant legislation (...), 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 country or by that international organisation, as well as the existence of effective and enforceable<sup>11</sup> data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred(...)<sup>12</sup>;

---

<sup>3</sup> AT, LU and FR expressed their support for maintaining the adequacy procedure. Some delegations raised concerns on the time taken up by adequacy procedures. LV thought a separate paragraph setting.

<sup>4</sup> CZ 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.

<sup>5</sup> IT, SK and AT scrutiny reservation.

<sup>6</sup> ES proposal.

<sup>7</sup> NL thought a preponderant role should be given to the EDPB in assessing these elements. COM indicated that this could be done in the articles dealing with the EDPB competences and that at any rate the Member States were involved in the adequacy procedure.

<sup>8</sup> CZ and IT asked for involvement of the EDPB.

<sup>9</sup> PL proposal. IT thought the list should not be exhaustive and therefore proposed adding 'in particular'.

<sup>10</sup> GR, AT and SK thought a reference to human rights should be inserted.

<sup>11</sup> ES proposal.

<sup>12</sup> Deleted further to CZ and FI remark that no distinction should be made between EU citizens.

(b) the existence and effective functioning of one or more independent<sup>13</sup> supervisory authorities<sup>14</sup> in the third country, or to which an international organisation is subject, with responsibility 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 concerned has entered into<sup>15</sup> in relation to the protection of personal data<sup>16</sup>  
17

3. The Commission, after assessing the adequacy<sup>18</sup> of the level of protection, 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. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure<sup>19</sup> referred to in Article 87(2).<sup>20</sup>

---

<sup>13</sup> Further to FDE and BE proposal.

<sup>14</sup> CZ and NL queried how strict this independence would need to be assessed.

<sup>15</sup> CH and NL remarked that many of these elements need to be formulated less broadly. FR thought the criteria should be more focused on implementation.

<sup>16</sup> CZ proposal. COM had clarified that this was mainly the CoE Convention No 108..

<sup>17</sup> DE proposed adding 'participation in a suitable international data protection system established in third countries or a territory or a processing sector' and 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). It also suggested referring to 'ways of ensuring consistent interpretation and application of the data-protection provisions under Articles 55 et seq'.

<sup>18</sup> DE proposal. CZ 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.

<sup>19</sup> BE and LU queried whether Member States would initiate such procedure.

<sup>20</sup> 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.



- 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*<sup>21</sup>.
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.
5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation no longer<sup>22</sup> 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).<sup>23</sup>
6. *Without prejudice to Articles 42 to 44, where (...) a decision is taken pursuant to paragraph 5, (...) transfers of personal data to the third country, or the territory or (...) processing sector within that third country, or the international organisation in question shall be prohibited (...). 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.*<sup>24</sup>

---

<sup>21</sup> Moved from paragraph 8. CZ and AT thought an absolute time period should be set. NL, PT and SI thought this paragraph 8 was superfluous or at least unclear. If maintained it should be moved to the end of the Regulation.

<sup>22</sup> COM reservation on the deletion of its possibility to adopt negative adequacy decisions.

<sup>23</sup> BE, DE, FI, IT, LU and FR asked for the deletion of paragraph 5.

<sup>24</sup> BE, DE, FR, FI, IT, LU and CZ asked for the deletion of paragraph 6.

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.
8. (...) <sup>25</sup>

*Article 42*

***Transfers by way of appropriate safeguards***<sup>26</sup>

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a recipient or recipients in a third country or an international organisation only if the controller or processor has adduced appropriate safeguards<sup>27</sup> with respect to the protection of personal data (...).
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular<sup>28</sup>, by:
- (a) binding corporate rules pursuant to Article 43; or
  - (b) standard data protection clauses adopted by the Commission<sup>29</sup> (...) in accordance with the examination procedure referred to in Article 87(2); or

---

<sup>25</sup> Move to paragraph 3a.

<sup>26</sup> Several delegations (BE, CH, IT) queried whether this article (in particular paragraphs 2 (a + b) and 5) could also be applied to public authorities. 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.

<sup>27</sup> SK scrutiny reservation.

<sup>28</sup> COM emphasised the non-exhaustive nature of this list, clarifying that also other types of agreements could be envisaged.

<sup>29</sup> FR reservation.

- (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2)<sup>30</sup>; or
  - (d) contractual clauses between the controller or processor and the recipient of the data<sup>31</sup> authorised by a supervisory authority pursuant to paragraph 4; or
  - (e) a certification mechanism pursuant to Article 39.<sup>32, 33</sup>
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.
  4. Where a transfer is based on contractual clauses as referred to in point (d)<sup>34</sup> of paragraph 2 (...) <sup>35</sup>, the controller or processor<sup>36</sup> shall obtain prior authorisation of the contractual clauses (...) from the competent supervisory authority (...).
  5. <sup>37</sup>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 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. (...).

---

<sup>30</sup> DE proposal.

<sup>31</sup> BE proposed referring to a sub-processor..

<sup>32</sup> NL proposed adding a reference to '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'.

<sup>33</sup> COM scrutiny reservation subject to assessing the final outcome of the compromise rules on certification mechanism.

<sup>34</sup> BE proposed adding a reference point (e).. CH thought this paragraph should not be applicable to public authorities.

<sup>35</sup> ES suggested inserting a reference to the absence of a DPO or certifications.

<sup>36</sup> BE suggested deleting the reference to the processor.

<sup>37</sup> BE and GR want to limit the scope of this paragraph to public authorities. IT on the contrary could not see how it could be applied by public authorities.

- 5a. If the transfer referred to in paragraph 4 or 5 is related to processing activities which concern data subjects in several Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.
- 5b. *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*<sup>38</sup>
6. (...) <sup>39</sup>.

*Article 43*

***Transfers by way of binding corporate rules***<sup>40</sup>

1. The competent supervisory authority shall *approve*<sup>41</sup> *binding corporate rules* in accordance with the consistency mechanism set out in Article 58 (...) provided that they:

---

<sup>38</sup> 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. The question as to the fate of existing MOUs and international conventions was also raised. AT, PL, GR, SI and BG voiced concerns regarding the possibility to transfer personal data in the absence of a legally binding instrument. FR scrutiny reservation on the terms 'administrative arrangements' and 'substantially affect the free movement of personal data'. BE also thought this paragraph needed clarification.

<sup>39</sup> Subsumed under paragraphs 4 and 5.

<sup>40</sup> Several delegations supported this innovative legal technique: BE, CZ, DE, FR, FI, IT, LU, NL, PT and PL. NL thought it should be given a wider scope. NL and GR pleaded in favour of covering data flows in the context of cloud computing and ES thought more flexibility should be provided in this way. SI thought it 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.

<sup>41</sup> 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.

- (a) are legally binding and apply to, and are enforced by, every member concerned<sup>42</sup> of the group of undertakings or group of enterprises engaged in a joint economic activity<sup>43 44 45</sup>;
  - (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data<sup>46</sup>;
  - (c) fulfil the requirements laid down in paragraph 2.
2. The binding corporate rules referred to in paragraph 1 shall at least<sup>47</sup> specify the following elements:
- (a) the structure and contact details of the group concerned<sup>48</sup> and each of its members<sup>49</sup>;
  - (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;

---

<sup>42</sup> DE proposal.

<sup>43</sup> Further to GR proposed to insert a reference to 'alliances'. BE proposed to refer to sub-processors; ES proposed to insert a reference (in paragraph 1(a) as well as in (2)(f)(h)(i) and (k) to 'business partners'.

<sup>44</sup> NL asked whether the BCRs should also be binding upon employees. ES thought subparagraph (a) could be simplified by stating that BCRs all binding to all involved.

<sup>45</sup> COM has a scrutiny reservation on 'group of enterprises engaged in a joint economic activity' extending the scope beyond one group of undertakings and how this would work in practice.

<sup>46</sup> FI proposed referring to BCRs and BE suggested a reference to effective administrative and judicial redress.

<sup>47</sup> FR pleaded in favour of deleting the words 'at least'. IT is opposed to the deletion thereof.

<sup>48</sup> BE proposals.

<sup>49</sup> BE proposal; BE also proposed a reference to sub-processors.

- (d) application of the general data protection principles, in particular purpose limitation, including the purposes which govern further processing<sup>50</sup>, 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<sup>51</sup> 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;
- (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, including monitoring (...) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

---

<sup>50</sup> NL proposal.

<sup>51</sup> FI proposal.

- (hh) the complaint procedures;
- (i) the mechanisms within the group (...) for ensuring the verification of compliance with the binding corporate rules<sup>52</sup>;
- (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.

- [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.]<sup>53</sup>
- 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).

---

<sup>52</sup> NL proposed referring to auditing as an example.

<sup>53</sup> CZ, IT, SE and NL reservation. FR scrutiny reservation regarding (public) archives. COM scrutiny reservation.

*Article 44*

***Derogations for specific situations***<sup>54</sup>

1. In the absence of an adequacy decision pursuant to Article 41, or of appropriate safeguards pursuant to Article 42<sup>55</sup>, a transfer or a category of transfers<sup>56</sup> 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

---

<sup>54</sup> EE, FR and NL reservation. UK thought that in reality these 'derogation' would become the main basis for international data transfers. It also opined that by their nature (many of) these derogations should not be called as such because the data transfers for which they allow are both justified and necessary.

<sup>55</sup> BE and LU proposed adding a reference to BCRs.

<sup>56</sup> FR and PL scrutiny reservation on the term 'set of transfers'.



- (d) the transfer is necessary for *important reasons of (...) public interest*<sup>57</sup>; *this must be a public interest recognised*<sup>58</sup> *in Union law or in the national law of the Member State to which the controller is subject* ; or
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims<sup>59</sup>; or
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent<sup>60</sup>; 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<sup>61</sup>;]<sup>62</sup> or

---

<sup>57</sup> 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. FR and IT reservation on the (subjective) use of the concept of public interest. It thought that also here it should be clarified that this ground cannot justify massive and structural transfers of data. LU proposed deleting the word 'important'.

<sup>58</sup> According to DE 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.

<sup>59</sup> PL requested clarification on this subparagraph.

<sup>60</sup> In the view of the Presidency this also covers public health emergency situations.

<sup>61</sup> FI requested clarification of this subparagraph.

<sup>62</sup> The Presidency will request the Commission to explain the purpose of this provision.

- (h) the transfer *which is not large scale or frequent*<sup>63</sup>, is necessary for the purposes of legitimate interests pursued by the controller or the processor<sup>64</sup> 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<sup>65</sup>; <sup>66</sup>
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 (a), (b) and (c) of paragraph 1<sup>67</sup> shall not apply to activities carried out by public authorities in the exercise of their public powers.
5. (...).<sup>68</sup>
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 (...) <sup>69</sup>.

---

<sup>63</sup> NL proposal. DE and SK also thought the terms 'frequent or massive' are unclear. UK thought this qualification should be deleted.

<sup>64</sup> FR requests clarification concerning the concept of "legitimate interest(s)" and would like the balance of Directive 95/46 to be preserved. It scrutiny reservation. AT, PT and PL are opposed to this subparagraph and plead in favour of its deletion.

<sup>65</sup> IT suggested deleting the words 'where necessary'.

<sup>66</sup> DE proposed adding another exemption in cases where the competent supervisory authority has granted prior authorisation. DE is of the opinion: 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.

<sup>67</sup> COM scrutiny reservation on deleting (h).

<sup>68</sup> Moved to paragraph (1)(d). DE and NL proposed adding the possibility of Member State law preventing a transfer of data outside the EU.

<sup>69</sup> GR reservation: GR suggested deleting this paragraph in view of the administrative burden it entailed for controllers. IT wanted to clarify the notification took place before the transfer.

[6a International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Directive 95/46/EC, shall remain in force until amended, replaced or revoked.]<sup>70</sup>

7. (...) <sup>71</sup>.

*Article 45*

***International co-operation for the protection of personal data***<sup>72</sup>

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<sup>73</sup>;
  - (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.

---

<sup>70</sup> COM enters scrutiny reservation based on strong legal doubts on the legality of such proposal. COM recalls recital 79 which states that ‘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 subject.’

<sup>71</sup> Deleted further to reservation by BE, CZ, CY, ES, FR, FI, SE and UK.

<sup>72</sup> PL thought (part of )Article 45 could be inserted into the preamble. 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.

<sup>73</sup> AT and FO thought this subparagraph was unclear and required clarification.

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries and international organisations, including their supervisory authorities, in particular where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3)<sup>74</sup>.

*Article 66*

***Tasks of the European Data Protection Board***

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:
  - (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;
  - (b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;
  - (c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;
  - (d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;
  - (dd) give an opinion on the level of data protection in third countries or international organisations;

---

<sup>74</sup> NL suggested deleting this paragraph.