Council of the European Union

Brussels, 12 September 2014
(OR. en)

13187/14

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 120
JAI 674
MI 656
DRS 113
DAPIX 120
FREMP 155
COMIX 459
CODEC 1811

NOTE

From:	French delegation
To:	Working Party on Information Exchange and Data Protection
No. prev. doc.:	11715/14 DATAPROTECT 102 JAI 594 MI 541 DRS 97 DAPIX 100 FREMP 141 COMIX 371 CODEC 1596
Subject:	Note from the French authorities on the proposal for a Data Protection Regulation – certification mechanism, including for transfers outside the European Union

In a note sent last July (ST 11715/14), the French authorities set out the general principles behind the certification mechanism for data controllers and processors not established in the EU and wishing to benefit from data transfers from the EU.

As stated in our note, we would like to present our drafting proposals concerning the mechanism so that they can be discussed by the DAPIX working party. We are also suggesting some drafting changes to Articles 39 and 39b regarding the certification mechanism in general.

The proposed drafting changes to Articles 39 and 39a, and a new Article 39c are set out below, with changes highlighted in bold

_____

ANNEX

Suggested drafting changes regarding the certification mechanism for data controllers and processors not established in the EU and wishing to benefit from data transfers from the EU

Article 39 Certification

1. The Member States, the European Data Protection Board and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with this Regulation by controllers and processors **subject to this Regulation**. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51.

3. The controller or processor which submits its processing to the certification mechanism shall provide the body referred to in Article 39*a*(1) with all information and access to its processing activities which are necessary to conduct the certification procedure.

4. The certification **shall be** issued to a controller or processor **for a maximum period of [three years] and may be renewed on the same conditions for as long as the controller or processor meets** the requirements for certification.

5. **The European Data Protection Board shall be notified of certifications issued and shall keep a public register of certified controllers and processors. The register shall be available on the European e-justice portal. The European Data Protection Board shall also be notified when certification is withdrawn so that it can update the public register of certified controllers and processors.**

Article 39a Certification body and procedure

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification **shall** be carried out by an **accredited** certification body **which is established in one or more Member States and** which has an appropriate level of expertise in relation to data protection.

2. The body referred to in paragraph 1 may be accredited for this purpose if:

(a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
(b) it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;
c) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;
d) it (…) demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The **European Data Protection Board shall draw up a reference framework on the basis of which the supervisory authorities shall examine accreditation requests.**

3a. **The body referred to in paragraph 1 shall be accredited by the European Data Protection Board on a proposal for accreditation, prepared by the supervisory authority of the Member State if the body has a single establishment and otherwise by the supervisory authority of the Member State in which the body has its registered office. The certification shall be issued for a maximum period of [three years] and can be renewed on the same conditions for as long as the body meets the requirements for certification.**

4. The body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification**,** without prejudice to the responsibility of the controller or processor for compliance with this Regulation.

4*a*. **Without prejudice to the provisions of Chapter VIII, the** body referred to in paragraph 1 shall, **subject to adequate safeguards, in cases of inappropriate use of the certification or where the requirements of the certification are not, or no longer, met by the controller or processor, withdraw the certification and notify the national supervisory authority referred to in paragraph 1 and the EDPD of the withdrawal.**

5. **The supervisory authorities shall regularly review the bodies referred to in paragraph 1. Those bodies** shall provide the competent supervisory authority with the **details of certifications issued and withdrawn** and the reasons for withdrawing the **certification. The supervisory authorities may require all relevant information to be communicated.**

6. The certification details shall be made public by the supervisory authority in an easily accessible form. **The European Data Protection Board shall keep a public register of accredited certification bodies. The register shall be available on the European e-justice portal.**

6*a*. **Any** competent supervisory authority **may submit to the European Data Protection Board a draft decision** to revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation. **When the European Data Protection Board revokes accreditation, it shall update the public list referred to in paragraph 6. The supervisory authority may propose that the European Data Protection Board request that the grounds for the revocation be entered in the margin of the public register kept by the European Data Protection Board and/or that a re-accreditation ban be imposed on the body concerned for a maximum period of five years.**

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of (…) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1.

7a. The European Data Protection Board shall give an opinion to the Commission on the criteria and requirements referred to in paragraph 7.

8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognise certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

New Article 39b - Certification of non-EU controllers or processors for data transfers from the EU

1. For the purposes of Article 42(2)(e), controllers or processors established exclusively in third countries, without any establishment in the EU, and wishing to receive transfers of personal data from controllers or processors who are subject to this Regulation, shall be required to undergo certification attesting that they at least meet the requirements referred to in paragraph 3 of this article for the processing of data including or intended to include the personal data of EU residents.

2. The rules laid down in Articles 39 and 39a on the accreditation of certification bodies, certification of controllers and processors established in third countries, and supervision of certified undertakings and certification bodies shall apply.

3. The certification bodies referred to in Article 39a(1), and accredited by the European Data Protection Board pursuant to Article 39a, may grant certification to controllers or processors not established in the territory of the EU provided that the recipients of data transfers expressly confer enforceable rights on data subjects with regard to the processing of their personal data and comply with legally binding rules which shall include at least provisions regarding:

(a) general data protection principles, including fair and transparent data processing, purpose limitation, data storage periods and sensitive data requirements;

(b) the information to be given to data subjects;

c) the exercise of data subjects' rights, including the right of access, the right to rectification and the right to be forgotten, the right to data portability, and the right to object;

d) data protection by design and default, measures and procedures to ensure the security of processing;

e) the notification of data breaches to the accredited body and the communication of data breaches to the controller or processor which initially transferred the data from within the EU;

f) onward data transfers to third countries or international organisations;

g) the mechanisms put in place within the undertaking to ensure verification of compliance with the legally binding rules provided for under this paragraph. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of the verification should be communicated to the data subject and should be available upon request to the accredited body or competent European supervisory authority;

h) the mechanisms for reporting and recording changes to the legally binding rules provided for under this paragraph and for reporting those changes to the accredited body or, upon request, to the competent European supervisory authority;

i) the mechanism for cooperation with the accredited body or competent European supervisory body to ensure that all of the undertaking's entities comply with the legally binding rules provided for under this paragraph, in particular by making the results of the verifications of the measures provided for in point (f) of this paragraph available to the accredited body or, upon request, to the competent European supervisory authority;

j) the appropriate data protection training for staff having permanent or regular access to personal data (...).

4. The accredited body granting certification under this Article to a controller or processor not established in the territory of the EU shall transfer the name and contact details of the certified undertaking as well as any other relevant information regarding the controller or processor to the national supervisory authority referred to in paragraph 1, and to the European Data Protection Board. The European Data Protection Board shall keep a public register of controllers and processors certified under this Article. The register shall be available on the European e-justice portal.

5. The European Data Protection Board shall introduce a European reference framework specifying the requirements laid down in paragraph 3 allowing controllers or processors established in third countries to obtain certification under this Article. The reference framework shall be updated as necessary and at least every five years.

5a. The Commission may specify the data security requirements provided for in point f) of paragraph 3. The corresponding implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

6. Data subjects may lodge a complaint with their supervisory authority and if necessary with the courts of their Member State of residence, against any controllers or processors certified under to this Article to whom their personal data have been transferred.