6733/13

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 21
JAI 131
MI 132
DRS 35
DAPIX 31
FREMP 16
COMIX 112
CODEC 399

NOTE

from:	Spanish delegation
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3 COMIX 40 CODEC 155
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Certifications

1. Introduction

One of the fundamental axes of the Spanish position is to promote policies that strengthen the levels of awareness and the capacities of the actors involved in the personal data processing operations.

The goal is not only to improve the quality and the privacy protection level, but also to find solutions that allow making the bureaucratic and administrative requirements more flexible and leaving at the same time room for auto-organization by introducing systems based on accountability.

Excellence and accountability would then be the two main pillars of a sound legal framework for certifications and its associated policies.

2. Legal framework and associated policies

At this stage only one article of the draft General Regulation on Data Protection is devoted to certifications. From our point of view, Article 39 is a good basis on which to make real progress towards the above-mentioned goals.

Nevertheless, we propose some amendments in order to strength the idea of polices linked to certifications, to associate certifications to specific benefits or options granted in the regulation, and to consider the Board as the centre of gravity at European level of the whole system. Additionally, it is important to empower national authorities as implementing and coordinating level.

Article 39
Certification

1. The **European Data Protection Board** ~~Member States and the Commission~~ shall encourage~~, in particular~~ at European level, the establishment of data protection certification **policies** ~~mechanisms~~ and of data protection seals and marks, allowing data subjects **and different actors** to quickly assess the level of data protection provided by controllers and processors. The data protection certification ~~mechanisms~~ **policies** shall contribute to the proper application of this Regulation, **and to obtain the options and benefits derived from it**, taking account of the specific features of the various sectors and different processing operations.

The European Data Protection Board, with the participation of other relevant actors, shall establish guidelines with regard to the certification policies at EU level.

The certification policies shall pay attention to the specific needs of the actors involved in the different sectors of activity, including public sector and specially taking into account the requirements of micro, small and medium sized enterprises, and the necessary cost containment to make these policies effective. The obtaining, renewal or loss of the certifications will produce the legal consequences provided by this Regulation.

2. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying~~ **T**he **policies shall establish** criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting**,** withdrawal, **expiration**, and requirements for recognition within the Union and in third countries.

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

2a **The supervision authorities shall be responsible at national level for coordinating and supervising the implementation of the certification polices.**

3. Associated benefits

When it comes to certifications one of the main weaknesses of the regulation is the lack of legal benefits associated to them.

According to this approach it is difficult to encourage the establishment of data protection certifications.

Of course, the first and one of the most important benefits of a certification is the confidence it creates to different stakeholders and public in general. That's why one of the key elements of a certification policy are the seals and marks associated and protected by it, which are already mentioned in Article 39. But this is not *sensu stricto* a legal benefit.

From our prospective, the following legal benefits could be envisaged for the draft regulation:

- Art. 22.1 There should be a clear statement indicating that having proper and valid certifications, according to Article 39, raises a rebuttable presumption of full compliance.

- Art. 26 There should be a clear statement allowing processors to provide the requested guarantees through proper certifications and associated seals.

- Art. 42.2 (d) and 42.4 and 5: Prior authorization should not be mandatory if the institution has a proper level of certification dealing with international transfers.

- Art. 79 Sanctions
  - Obtaining a proper certification could be considered as one of the possible corrective actions that could avoid being fined (see our non-paper on sanctions)
  - Having a certification could be considered as a mitigating factor in non-intentional first infractions.
  - Part of the sanction could be withdrawal or temporary restraining of the certification

Additionally depending on the solutions applied to the prior consultation issues, certifications could be a good way to go as well.

Concerning Article 28 we expect more appropriate solutions could be found, in the line of the Presidency's working document on administrative burdens. If it is the case, on the basis of simplifying requests and giving way to more accountability friendly expressions like "giving documentary evidence", we could study removing our certifications-based amendments for this provision.

4.   Key elements of the certification's policy

- **Rigorous concession**. The obtaining of a certification will require overcoming several objective tests, to prove the fulfilment of the necessary requisites linked to its definition. The content of the tests, and therefore, of the preparation programmes or courses, should combine legal with technical issues. The weight of each of these elements would vary depending on the kind of certification, the institution or staff targeted.

- **Temporality.** Each certification will be subject to a caducity deadline, which will vary depending on the kind of certification. The certification should be renewed before expiring. To this end, the necessary tests to objectively prove that the organization or person's capacities are the same or have improved should be established.

- **Revocability**. Every certification could be revoked as a consequence of relevant breaches. The definition of breaches, the procedure for revoking and the possibility of preventative revoking should be established by the Regulation.

- **Flexibility.** Certifications policy should offer different kind of products according to different sectors and subsectors needs. The starting point should be that only those capacities really needed for a certain processing operation should be certified. Nobody should be compelled to certify activities that are not comprehended in their corporative or organizational duties. This way, the prices of the certification policy would be substantially cut.

- **Quality**. The certification policy should obey to quality criteria. To achieve this goal, quality control programmes from design and use should be developed.

- **Planning.** The certification policy should adapt to a reality that is in constant change. Therefore, these policies should include a planning and development team that detects the new needs and propose operative and efficient responses.

_____