European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

2009/0089(COD) - 15/06/2011

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Carlos COELHO (EPP, PT) on the amended proposal for a regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

The committee recommends that the European Parliament's position in first reading following the ordinary legislative procedure make certain amendments to the Commission proposal. A large number of the amendments relate to improvements in terms of security and data protection and the role of the European Parliament, as well as transparency. There are special provisions for the participation of Denmark.

The main amendments are as follows:

The Agency: the committee made it clear that the Agency may only be made responsible for the preparation, development and operational management of other large-scale IT systems in the area of freedom, security and justice, **only if so provided by the relevant legislative instrument, based on Title V of the Treaty on the Functioning of the European Union (TFEU).** Operational management shall consist of all the tasks necessary to keep the large-scale IT systems functioning in accordance with the specific provisions applicable to each of those large-scale IT systems, including responsibility for the communication infrastructure used by the large-scale IT systems. Those systems shall not exchange data and/or enable sharing of information and knowledge, unless provided in a specific legal basis.

The report notes that in the joint statements accompanying the SIS II and VIS legal instruments, the European Parliament and the Council invited the Commission to present, following an impact assessment, the necessary legislative proposals entrusting an Agency with the long term operational management of the Central SIS II and parts of the communication infrastructure as well as the VIS.

Objectives: the Agency shall ensure:(a)the implementation of effective, secure and continuous operation of the large-scale IT systems (b) the efficient and financially accountable management of those systems; (c) an adequately high quality of service for users of those large-scale IT systems;(d) continuity and uninterrupted service;(e) a high level of data protection, in accordance with the applicable rules, including specific provisions for each large-scale IT system (f) an appropriate level of data– and physical security, in accordance with applicable rules, including specific provisions for each of the large-scale IT systems and; (g) the use of an adequate project management structure for efficiently developing large-scale IT systems.

Tasks: Members specify that the core mission of the Agency is to fulfil the operational management tasks for SIS II, VIS and EURODAC and, if so decided, other large-scale IT-systems in the area of freedom, security and justice. The Agency should also be responsible for **technical measures** required by the tasks entrusted to it, which are not of a normative nature. These responsibilities should be without prejudice to the normative tasks reserved to the Commission alone or assisted by a Committee in the respective legal

instruments governing the systems operationally managed by the Agency. In addition, the Agency should perform tasks related to **training on the technical use** of SIS II, VIS and EURODAC and other large-scale IT systems which might be entrusted to it in the future.

Members stress that the Agency might also be made responsible for the preparation, development and operational management of additional large-scale IT systems in application of Title V of the TFEU, but only by means of subsequent and separate legal instruments, preceded by an impact assessment.

A new clause is inserted on **tasks related to the communication infrastructure**, which specifies that the Agency shall carry out the tasks relating to the communication infrastructure conferred on the Management Authority by the legal instruments governing the development, establishment, operation and use of the large scale IT systems.

According to those legal instruments, the tasks regarding the communication infrastructure (including the operational management and security) are divided between the Agency and the Commission. In order to ensure coherence between the exercise of the respective responsibilities of the Commission and the Agency, operational working arrangements shall be made between them and reflected in a Memorandum of Understanding. Appropriate measures including security plans shall be adopted. The tasks concerning the operational management of the communication infrastructure **may be entrusted to external private-sector entities or bodies but the network provider shall be bound by the security measures and shall not have access** to VIS, EURODAC and SIS II operational data and the related SIRENE exchange by any means.

Lastly, the Agency should be responsible for **monitoring of research and for pilot schemes**, in accordance with the provisions of Council Regulation (EC, Euratom) No 1605/2002 on the Financial, for large-scale IT systems in application of Title V of the TFEU, at the specific and precise request of the Commission. When tasked with a pilot scheme, special attention should be given to the European Union Information Management Strategy.

Seat: the seat of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice will be **Tallinn, Estonia**. The tasks related to development and operational shall be carried out in **Strasbourg, France**. A backup site capable of ensuring the operation of a large scale IT system in the event of failure of that system shall be installed in **Sankt Johann im Pongau, Austria**, if so provided in the legislative instrument governing the development, establishment and use of that system.

The recitals note that as was agreed, the seat of the Agency should be in Tallinn (Estonia). However, since the tasks related to technical development and the preparation for the operational management of SIS II and VIS were already carried out in Strasbourg (France) and a backup site for these IT systems was already installed in Sankt Johann im Pongau (Austria), this should continue to be the case. These two sites should also be the locations, respectively, where the tasks related to technical development and operational management of EURODAC should be carried out and where a backup site for EURODAC should be established. This should also be the case regarding, respectively, the technical development and operational management of other large-scale IT systems in the area of freedom, security and justice and a backup site capable of ensuring the operation of an IT system in the event of failure of that system, if so provided in the relevant legislative instrument.

Structure: the Agency's structure shall also include: (a) a Data Protection Officer; (b) a Security Officer; (c) an Accounting Officer.

Management Board: the list of members of the Management Board shall be published on the Agency's internet site.

Appointment of the Executive Director: the latter will be appointed for a period of five years from among the eligible candidates identified in an open competition organised by the Commission. This selection procedure will provide for publication in the Official Journal and elsewhere of a call for expressions of interest. The Management Board could require a repeated procedure if it is not satisfied with the suitability of any of the candidates retained in the first list. The Executive Director shall be appointed on the basis of his or her personal merits, experience in the field of large scale IT systems and administrative, financial and management skills as well as knowledge in data protection. The Management Board shall take the decision by a two-thirds majority of all members with a right to vote.

Advisory Group: Member States should appoint a Member to the Advisory Group concerning a large-scale IT system, if they are bound under Union law by any legislative instrument governing the development, establishment, operation and use of that particular system. Each country associated with the implementation, application and development of the Schengen acquis, the EURODAC-related measures and the measures related to other large scale IT systems which participates in a particular system shall appoint a member to the Advisory Group which concerns that system.

Access to documents:on the basis of a proposal by the Executive Director, and not later than six months after the entry into force of the Regulation, the Management Board shall adopt rules concerning access to the Agency's documents, in accordance with Regulation (EC) No 1049/2001.

Security of the Agency: this new provision states that the Agency shall be responsible for the security and the preservation of order within the buildings, premises and land used by it. The Agency shall apply the security principles and relevant provisions of the instruments governing the development, establishment, use and operation of the large-scale IT-systems. Furthermore, the host Member States shall take all effective and adequate measures to preserve order and security in the immediate vicinity of the buildings, premises and land used by the Agency and shall provide to the Agency the appropriate protection.

Evaluation: within three years from the date of the Agency having taken up its responsibilities, and every four years thereafter, the Commission, shall perform an evaluation of the action of the Agency examining the way and extent to which the Agency effectively contributes to the operational management of large-scale IT systems in the area of freedom, security and justice and fulfils its tasks described in the regulation. The evaluation should also evaluate the role of the Agency in the context of a Union strategy aimed at a coordinated, cost-effective and coherent IT environment at Union level that is to be established in the coming years. The Commission’s recommendations following the evaluation must be forwarded to the **European Data Protection Supervisor** as well as the Council and the European Parliament.

Fundamental rights: lastly, the text states that within the framework of their respective competences, the Agency should cooperate with other agencies of the EU, especially agencies established in the area of freedom, security and justice, and in particular the European Union Agency for Fundamental Rights. It should also consult and follow-up the recommendations of European Network and Information Security Agency regarding network security, where appropriate.