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

2009/0089(COD) - 05/07/2011 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 607 votes to 48, with 14 abstentions, a legislative resolution 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.

Parliament adopted its position at first reading, under the ordinary legislative procedure. The amendments adopted in plenary are the result of a compromise negotiated between the European Parliament and the Council.

They amend the Commission proposal as follows:

The Agency: Parliament 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. **These systems shall not exchange data and/or enable sharing of information and knowledge**, unless provided in a specific legal basis.

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: besides its core mission, 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.

New provisions are inserted on **tasks related to the communication infrastructure.** These tasks 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. 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.

Moreover, and only on the express request of the Commission, which shall have informed the European Parliament and the Council at least three months in advance, and after a decision by the Management Board, the Agency may, carry out **pilot schemes** for the development and/or the operational management of large-scale IT systems, in application of Title V of the TFEU. The European Parliament, the Council and, where data protection issues are concerned, the European Data Protection Supervisor shall be regularly kept informed of the evolution of these pilot schemes.

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. However, the tasks related to development and operational management 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.

Since the tasks relating to technical development and the preparation for the operational management of SIS II and VIS are already carried out in Strasbourg and a backup site for those IT systems has already been installed in Sankt Johann im Pongau, this should continue to be the case. Those two sites should also be the locations, respectively, where the tasks relating to technical development and operational management of Eurodac should be carried out and where a backup site for Eurodac should be established. It is, moreover, stipulated that the host Member States should provide the best possible conditions to ensure the proper functioning of the Agency, for example including multilingual, European-oriented schooling and appropriate transport connections.

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

Management Board: provisions are laid down to improve and strengthen the structure and operation of the Agency’s Management Board. Member States will have voting rights within the Agency’s Management Board if they are bound under Union law by a legislative instrument governing the development, establishment, operation and use of a large-scale IT system in question. Specific provisions are made to take account of the particular situation of Denmark in this regard.

Executive Director: it is stipulated that the Agency’s Executive Director should be appointed by the Management Board for a period of five years, from a list of eligible candidates identified in an open competition organised by the Commission. The candidate selected by the Management Board shall be invited to make a statement before the European Parliament which shall then adopt an opinion setting out its view of the selected candidate. The Management Board shall inform the European Parliament of the manner in which that opinion has been taken into account.

Advisory Group: each Member State which is bound under Union law by any legislative instrument governing the development, establishment, operation and use of a particular large-scale IT system, as well as the Commission, shall appoint one member to the Advisory Group which concerns that large-scale IT system , **for a three-year term, which may be renewed**. Denmark may also appoint a member if it decides to transpose the Regulation.

Security of the Agency: the Agency shall be responsible for the security and the preservation of order within the buildings, premises and land used by it. 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.

Financing: the financing of the Agency should be subject to an agreement by the budgetary authority (European Parliament and Council).

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.

Cooperation with other agencies: within the framework of their respective competences, the Agency should cooperate with other agencies of the Union, 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 the European Network and Information Security Agency (ENISA) regarding network security, where appropriate.