

Control of exports, brokering, technical assistance, transit and transfer of dual-use items

2016/0295(COD) - 17/01/2018 - Text adopted by Parliament, partial vote at 1st reading/single reading

The European Parliament adopted by 571 votes to 29, with 29 abstentions, **amendments** to the proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast).

The matter was **referred back to the committee responsible** for interinstitutional negotiations.

The main amendments adopted in plenary concern the following issues:

Cyber-surveillance and human rights violations: in addition to traditional dual-use items, the Regulation should cover cyber-surveillance assets used to directly interfere with human rights, including the **right to privacy and data protection, freedom of expression, freedom of assembly and association**.

Items to be covered by this Regulation should include hardware, software and technology, which are specially designed to enable the covert intrusion into information and telecommunication systems and/or the monitoring, exfiltrating, collecting and analysing of data and/or incapacitating or damaging the targeted system **without the specific, informed and unambiguous authorisation** of the owner of the data.

Considering the rapid advance of technological developments, it is appropriate that the Union introduces controls on certain types of cyber surveillance technologies on the basis of a unilateral list, in Section B of Annex I. The Council, the Commission and Member States should, in close cooperation with the EEAS, pro-actively engage in the relevant international fora in order to establish the list of cyber-surveillance items set out in Section B of Annex I as an **international standard**.

Due diligence: if an exporter, becomes aware while exercising due diligence that dual-use items not listed in Annex I which he or she proposes to export, may be intended to violate human rights, he or she must notify the competent authority of the Member State in which he or she is established or resident in, which will decide whether or not it is expedient to make the export concerned subject to authorisation.

A Member State may prohibit or impose an authorisation requirement on the export of dual-use items not listed in Annex I for reasons of public security, for human rights considerations or for **the prevention of acts of terrorism**. The manufacturer's note of licensing requirements should also be compulsory for exports to third countries.

Export authorisations: individual export authorisations and global export authorisations shall be valid for **two years**, and may be renewed by the competent authority. They may be suspended or revoked at any time. The identity or nature of the entity that will be the end-user shall be identified.

Applications for authorisation shall be processed within **30 days** of the filing of the application and the competent authority shall decide on applications for individual or global export authorisations, at the latest, within **60 days** of valid submission of the application.

The exporter shall have the possibility, on a voluntary basis, to have its internal compliance programme (ICP) certified free of charge by the competent authorities on the basis of a reference ICP established by the Commission, in order to obtain **incentives** in the authorisation process.

Criteria to be taken into account: in deciding whether or not to grant an individual or global export authorisation, the competent authorities of the Member States shall take into account all relevant considerations including:

- **the obligations of the Union and the Member States** under sanctions imposed by a decision or a common position adopted by the Council or by a decision of the OSCE or by a binding resolution of the Security Council of the United Nations;
- **the occurrence of violations of human rights law**, fundamental freedoms and international humanitarian law in the country of final destination as has been established by the competent bodies of the UN, the Council of Europe or the Union;
- **the behaviour of the country of destination** with regard to the international community, as regards in particular its attitude to terrorism, the nature of its alliances and respect for international law.

With regard to **cyber surveillance items**, the competent authorities of the Member States shall in particular consider the risk of violation of the right to privacy, the right to data protection, freedom of speech and freedom of assembly and association, as well as risks relating to the rule of law. If the existence of such risks is likely to lead to serious violations of human rights, Member States shall **not grant export authorisations**.

Guidelines: Members proposed that the Commission and the Council make guidelines available (in the form of a handbook) as soon as the Regulation enters into force, so as to ensure common risk assessments as well as uniformity of the criteria for licensing decisions.

That handbook shall be developed in close cooperation with the European External Action Service (EEAS) and the Dual Use Coordination Group and shall involve **external expertise** from academics, exporters, brokers and civil society organisations.

Modification of lists: new risks and new technologies may be added urgently to the Regulation. The Commission may also remove items from the list if, as a result of the fast-changing technological environment, these items have become lower tier or mass market products that are easily available.

Penalties: the Dual-Use Coordination Group shall set up an Enforcement Coordination Mechanism to provide for uniform criteria for licensing decisions. Upon assessment by the Commission of the rules on penalties laid down by Member States, the mechanism shall provide for ways to **make penalties for infringements of this Regulation similar in nature and effect**.

Transparency: Member States shall **disclose publicly, at least quarterly** and in an easily accessible manner, meaningful information on each license with regard to the type of license, the value, the volume, nature of equipment, a description of the product, the end user and end use, the country of destination, as well as information regarding approval or denial of the license request.

Lastly, Members asked that the Commission's evaluation report on the Regulation include a proposal on the **deletion of encryption technologies** from the list of controlled items.