



15 October 2026

DIGITALEUROPE's Contribution to the public consultation on the evaluation of the dual-use regulation

Executive summary

DIGITALEUROPE welcomes the opportunity to contribute to the European Commission's evaluation of the Dual-Use Regulation (Regulation (EU) 2021/821). The evaluation should ensure that the Regulation effectively delivers on its security objectives while preserving the EU's global competitiveness, supporting innovation and legitimate trade, reducing unnecessary administrative burdens, and promoting a harmonised and predictable export control framework across the EU. It should also assess whether the current framework remains fit for purpose in light of the evolving geopolitical and technological landscape.

In this context, DIGITALEUROPE provides recommendations that would strengthen the effectiveness, consistency and proportionality of the EU export control framework while supporting the objectives of the EU's Economic Security agenda.

In particular:

- ▶ **Multilateral frameworks help avoid the pitfalls of unilateral controls.** Commission Expert Groups should be used for EU internal alignment, while platforms such as the G7, EU-US cooperation frameworks, Pax Silica, High-Level Economic Dialogues, and other **partnerships with like-minded countries should be leveraged** for external coordination towards convergence of export controls.
- ▶ When extending export controls, **evaluation criteria should look at foreign availability, enforceability, impact on EU competitiveness, alignment with key partners, and likelihood of retaliatory responses.** Redundant controls of technologies that are now globally available, such as widely available mass-market commercial encryption, should be removed when possible.
- ▶ Economic security initiatives should **prevent overlap and complexity, ensuring coherent implementation of sanctions and export controls**, with clear guidance on their respective requirements. Existing tools should be reviewed before creating new regulatory structures.
- ▶ **Human rights impact and misuse potential should be considered when regulating cyber-surveillance items.** The Dual-Use Regulation should reflect the clarifications provided in the Commission guidelines published in October 2024, ensuring their consistent application across the EU.
- ▶ The Dual-Use Regulation's vague definitions for intangible transfers have created a patchwork of divergent national approaches, increasing costs for EU exporters, and leaving the EU at a competitive disadvantage. **Certainty for remote maintenance, diagnostics, software support and cybersecurity updates that rely on cross-border digital connectivity is essential.** To support a clear and consistent application of the existing framework, upcoming Commission





guidelines should clarify **how the Regulation's definition of 'export' applies to intangible transfers**, including that an export of controlled technology occurs only when the technology is decrypted and accessed outside the EU, and that the provision of SaaS does not in itself constitute an export of software.

- ▶▶ A **forum for political coordination on export controls should be established**, with private sector involvement and technical expertise.
- ▶▶ Enhanced cooperation between Member States and industry, supported by technical expertise, is essential. The Commission should **strengthen its internal expertise and establish formal expert groups with industry representation**.
- ▶▶ **Greater harmonisation** is also needed to facilitate compliance, including through an EU-wide mechanism for identifying excluded parties and countries that supports due diligence and enables greater automation.
- ▶▶ The use of **Union General Export Authorisations (UGEAs)** should be improved by **expanding the range of eligible destinations**, where appropriate, while maintaining proportionate and risk-based safeguards.



Table of contents

Executive summary	1
Table of contents	3
1. Clarity of implementation and stakeholder consultation.....	4
Consistent application of export controls in the EU	4
Structured stakeholder engagement and cooperation	4
2. Intangible technology transfers, non-listed items, cyber-surveillance items	5
Software and intangible technology transfers.....	5
Cybersurveillance items.....	6
3. Intra-EU transfers	6
Evaluation criteria: transparency, clarity of implementation and guidance	6
Critical technologies.....	7
Multiplication of legal instruments	8
4. Licensing	8
Expansion and harmonisation of EU general and global export authorisations.....	8
Level playing field for EU exporters in the Single Market & Internationally	9
5. Meeting current and future needs.....	9
Forum for political coordination on export controls	9
Overall assessment of the Dual-Use Regulation	9

1. Clarity of implementation and stakeholder consultation

Consistent application of export controls in the EU

We welcome the Commission's ambition for further harmonisation of controls across the EU. The uniform adoption of controls that were not developed through multilateral regimes would help avoid market fragmentation, as compared to unilateral and uncoordinated controls by certain member states.

However, we also note that the adoption of unilateral controls by the EU risks harming not only the global competitiveness of European industry, but the effectiveness of such controls. Unilateral controls pose challenges to both small and large companies and fragment the internal market.

The EU should continue to pursue multilateral approaches to export controls wherever possible. However, given that the current geopolitical context has constrained the ability of existing multilateral export control regimes, including the Wassenaar Arrangement, to deliver timely outcomes, the EU should strengthen coordination with trusted and like-minded partners. This would help develop coherent, effective and proportionate export controls, while minimising fragmentation and preserving a level playing field.

Following multilateral consultations, Member States, in collaboration with the Commission, should make use of the Commission Expert Groups to align and finalise such controls and de-controls prior to adoption. Moreover, the EU should also leverage other platforms to seek alignment with like-minded partners and industry stakeholders on this issue. Key coordination mechanisms should include the EU-US Digital Dialogue, Pax Silica, the G7, High-Level Economic Dialogues, and other coordination and partnerships with like-minded countries to promote convergent export control approaches.

Structured stakeholder engagement and cooperation

Outside the proposed political coordination forum, enhanced cooperation between Member States and industry remains necessary. We believe that technical expertise is required when deciding on new item controls.

To form a comprehensive understanding of the practical application of controls, the Commission should improve internal technical expertise, as well as leverage contributions from national authorities and industry. Stakeholder meetings must be scheduled on an ad-hoc basis to ensure broader stakeholder engagement, providing a platform for public consultation, valuable feedback and opportunities for industry insights with government stakeholders.

One good example of this type of cooperation is the use of technical advisory committees in partner jurisdictions, which grant a variety of stakeholders the opportunity to apply for a mandate to provide input to ongoing and upcoming initiatives via confidential sessions. These technical groups advise on export control policy on a broad range of goods, technologies and software presently controlled under the Wassenaar Arrangement for national security, foreign policy and non-proliferation purposes.

We recommend the Commission to take inspiration from these good practices and form expert groups, preferably with technical backgrounds, that are officially structured to include industry representatives and government officials. These expert groups would play a crucial role in offering guidance to the Commission on setting technical criteria for export controls on dual-use goods and technologies, as well as advising on the consistent application of these controls.

2. Intangible technology transfers, non-listed items, cyber-surveillance items

Software and intangible technology transfers

The definition of ‘export’ in the Dual-Use Regulation is ambiguous as it concerns the intangible transfer of software and technology. In particular, the concept of making data available in an electronic form is unclear in the Regulation. This has led to varied interpretations and regulations for such transfers both within the EU and in its dealings with global partners, complicating the export process and increasing costs for EU exporters. The lack of harmonised rules on software and technology transfers places EU exporters at a competitive disadvantage compared to their global counterparts.

In line with Recital 11 of the Dual-Use Regulation, which calls for general or global licences or harmonised interpretations for certain software and technology transfers, DIGITALEUROPE welcomes the Commission initiative to develop clear and harmonised guidelines in this area. Such guidelines would be a significant step towards reducing administrative burdens and legal uncertainty for exporters and national authorities.

DIGITALEUROPE’s position is set out here: [Proposed guidelines on export controls for intangible technology transfers - DIGITALEUROPE](#). Key elements of our position include:

- ▶ **Encrypted technology is only exported if decrypted and accessed outside the EU.** In other words, uploading controlled technology to a server outside the EU should not constitute a licensable export, provided the technology remains encrypted using recognised cryptographic standards (e.g., ISO/IEC 19790), and the means to access the technology (e.g., a decryption key) is not made available to a recipient outside the EU;
- ▶ **The provision of Software as a Service (SaaS) does not constitute a software export,** as the user does not access the underlying source code or object code. In a SaaS model, the software application, its source code, object code, binary executables, configuration logic, and all underlying technical, resides exclusively on infrastructure controlled by the SaaS provider. The user of the SaaS service never receives, downloads, installs, or otherwise obtains a copy of the software in any form. Without downloads and/or access to the source code or object code, the recipient is unable to replicate the controlled software, and the security risk that export controls seek to address does not materialise;
- ▶ **The responsible exporter is the user of an IT service, rather than the IT service or infrastructure provider.** The user is the party that decides whether to transmit controlled software or technology to recipients outside the EU. IT service or infrastructure providers do not have information about whether user content is controlled, nor do they decide where, when or to whom their users transmit data.
- ▶ **The national competent authority is the one applicable to where the exporter is located,** as defined in Art. 2(3)(b) Dual-Use Regulation, not where the electronic means server is located.

The Commission should also consider clarifying the application of export controls to remote maintenance and technical support, relying on cross-border digital connectivity, in line with the recommended approaches above. Specifically, the provision of technical support and maintenance services by personnel located outside the EU should not constitute an export, provided that controlled content remains encrypted or

otherwise inaccessible. This clarification should cover remote maintenance, diagnostics, software support and cybersecurity updates that rely on cross-border exchanges.

The ambiguities in the Dual-Use Regulation have also given rise to divergent national interpretations regarding remote access to controlled hardware. The Commission should clarify that the provision of remote access to controlled hardware located within the EU should not constitute an export, provided that no controlled software or technology is transmitted in accessible form to a recipient outside the EU. When controlled hardware is remotely accessed, the hardware remains in the EU, and the remote user does not gain possession or control of any controlled item.

Cybersurveillance items

We welcome the additional clarity provided by the Commission's 2024 Guidelines on the implementation of controls on cyber-surveillance items under Article 5. Should these provisions be reviewed in the future, we would encourage the Commission to maintain a proportionate and risk-based approach, taking into account technological developments and the need for legal certainty.

In this context, consideration could be given to:

- ▶▶ The positive human rights impact of the item, including the rights to privacy and personal security; and
- ▶▶ The misuse potential of an item in risk analysis, especially when the item, despite its risks, is unlikely to be used harmfully due to more effective alternatives.

We believe that certain items, potentially viewed as cyber-surveillance tools, do not pose a risk for use in internal repression or serious human rights and international law violations. In this context, the line between legitimate commercial functionality and cyber-surveillance capability is often not clearly defined. Technologies primarily intended for legitimate cybersecurity purposes should not be considered cyber-surveillance items solely because they include monitoring capabilities. Any future consideration of these provisions should continue to ensure sufficient clarity for legitimate commercial activities. The Commission should ensure that the clarifications provided in the October 2024 Guidelines are applied consistently across the EU.

3. Intra-EU transfers

Evaluation criteria: transparency, clarity of implementation and guidance

When considering the extension of export controls to new items, the Commission and Member States should consider the following key evaluation and selection criteria:

- ▶▶ The foreign availability of the item outside the EU;
- ▶▶ The ability to make a clear and objective specification of the item;
- ▶▶ The enforceability of the controls;
- ▶▶ The impact on EU competitiveness;
- ▶▶ The impact on trusted cross-border research and industrial cooperation;

- 
- ▶▶ The impact on trusted European collaborative programmes, including EU-funded research, innovation and defence initiatives, where excessive administrative requirements could unnecessarily hinder secure cross-border cooperation between established participants;
 - ▶▶ The extent of alignment with key partners on similar or comparable controls;
 - ▶▶ The likelihood of retaliatory responses from third countries;
 - ▶▶ The risk profile of the relevant end-use/end-user to differentiate high-risk strategic technologies from low-risk activities (risk-tiered model).

There is also a clear risk that there will be export controls in different countries and regions seeking to achieve the same goals by different means. This will make it more difficult and resource-consuming for global industries to comply with export controls than under current identical (or at least very similar) export controls.

As export control compliance frameworks become increasingly complex, Member States and the Commission should consider removing existing controls where possible. Continuing to control technologies that are now globally and widely available to the public such as Cryptography Note 3 items is ineffective, and listed technologies should be regularly evaluated to ensure controls remain proportionate and do not unnecessarily restrict collaboration with trusted partners on critical technologies. Therefore, the framework applicable to widely available mass-market products should be regularly evaluated to reduce unnecessary administrative burdens and ensure that any remaining controls are effective and proportionate.

Critical technologies

The EU's Economic Security Strategy and the EU's evolving economic security framework have further reinforced the identification and assessment of critical technologies as a cornerstone of EU economic security policy. We underline the importance of stakeholder engagement throughout the assessment process: relevant industry actors should be able to share real time feedback on their product development practices and other regimes they are having to comply with.

Controls on critical technologies might prove challenging to implement, and impact negatively on supply chains. In this context, we emphasise the importance of recognising that not all advanced technologies pose a risk of civil-military fusion. Should the Commission consider expanding controls to new critical technologies, besides the evaluation criteria outlined in the previous section, it should also take into consideration that regulating the fast-changing and varied technology sector with methods mainly designed for stable and traditional fields, such as export restrictions on specific materials, can lead to a system that does not match the pace of advancements and is too slow and cumbersome. This is especially true for critical technologies that are still in early stages of development.

Controls on critical technologies should be sufficiently technology-neutral and adaptable to keep pace with technological developments and avoid unintended distortions between different technological approaches.

Given the importance of cross-border research and development and standardisation initiatives for technological innovation, we recommend that any future new controls on critical technologies be complemented with EU-level or national general authorisations that allow for continued cooperation between trusted partners.



Where appropriate and without compromising security objectives, simplified or general authorisation mechanisms should also facilitate technology transfers between established entities participating in trusted European collaborative programmes and consider trusted exporter approaches for companies demonstrating mature Internal Compliance Programmes, robust screening systems, auditability and established compliance governance. This would facilitate lower-risk transactions while preserving effective controls and strengthen the competitiveness of the European Defence Technological and Industrial Base.

Multiplication of legal instruments

The Commission and Member States should consider economic security initiatives carefully to avoid overlap, inconsistencies and unnecessary complexity.

The evolving EU economic security framework should avoid overlap between the laws governing sanctions and export controls. It is crucial to distinguish their respective legal bases and objectives while ensuring coherent implementation, even though they may be monitored and implemented by the same government authorities at the Member State level.

In addition, existing export-control tools should be reviewed and their effectiveness fully assessed before new regulatory structures are introduced to address related concerns.

4. Licensing

Expansion and harmonisation of EU general and global export authorisations

The Commission should strive to expand its general export authorisations to account for new technologies and partnership with like-minded countries. The EU should recognise allied countries with comparable controls as trusted partners eligible for exports under general export authorisations.

For example, countries that are eligible for most EU general export authorisations should be incorporated into EU001, which allows exports of most dual-use items to a defined group of trusted destinations without requiring an individual export licence. In addition, given the widespread commercial availability of several encryption-related technologies, the EU should consider broadening EU008 to cover key trade partners that pose a materially lower risk than other excluded countries.

Where several Member States have national general export authorisations in place, the EU should establish an EU general export authorisation that matches the license scope of national authorisation. This would level the playing field for EU exporters and simplify overall licensing options.

Further alignment is also needed in the implementation of global export authorisations, where practices continue to differ across Member States. A more harmonised EU approach should enable global authorisations to be granted at control-code and destination-country level with consistent terms, procedures and reporting requirements across Member States.

Additional work is also needed towards the interoperability and digitalisation of national licensing systems. A move towards standardised digital licences and harmonized procedural mechanisms would reduce administrative burdens, enable greater automation of compliance processes, and support more efficient cross-border operations.

Level playing field for EU exporters in the Single Market & Internationally

The existing system of EU and National General Export Authorisations (UGEAs and NGEAs), which recognises trusted jurisdictions, has been a key driver of cross-border innovation. We recommend further streamlining and simplifying eligibility conditions to facilitate technological advancement with other trusted partners on a global scale.¹

While UGEAs provide important benefits to EU exporters, their scope and flexibility remain more limited than comparable general authorisations and licence exceptions available in some partner jurisdictions. This places EU exporters at a competitive disadvantage.² We therefore recommend the Commission examine practices in partner jurisdictions and identify opportunities to further broaden and expand UGEAs, helping to close this gap and ensure a more level playing field.

Alongside these efforts, closer international cooperation with likeminded countries, including through the G7 and the EU-US Digital Dialogue, facilitated by coordination of controls, licensing policies, enforcement and interoperability, leveraging existing, well understood concepts in the EU export control regime would be beneficial. In particular, the Commission should seek to coordinate the adoption of new controls on critical technologies amongst Member States and trusted international partners, ensuring timely publications, standardised export control classification codes, consistent licensing policies, and sufficient time between publication and controls coming into effect.

5. Meeting current and future needs

Forum for political coordination on export controls

The proposal in the Commission's Export Control White Paper to establish a forum for political coordination on export controls is welcome. This forum should also actively solicit contributions from the private sector and have technical experts on board to ensure a comprehensive approach to export controls, including by considering having dedicated expert groups for individual critical technologies. In addition, coordination with likeminded partners is paramount to avoid unilateral restrictions.

If the EU plans to extend export controls to include emerging and new technologies not currently covered by export controls, it is crucial to involve industry through wide-ranging and ongoing consultations. This would help ensure controls are well targeted and implementable. To gather essential input from industry, establishing technical expert groups under Art. 24 of the Dual-Use Regulation should be considered. These groups should include not only Member State experts but also representatives from relevant industry sectors.

Overall assessment of the Dual-Use Regulation

The evaluation of the Dual-Use Regulation provides an opportunity to assess how the current framework is functioning in practice and whether it remains effective, proportionate and responsive to today's security challenges while preserving Europe's competitiveness and innovation capacity. The deterioration in the

¹ As an example of this, we welcome the UK Export Control Joint Unit's open export general licence to cover exports of chip and quantum technologies to the EU and other trusted partners.

² For example, the U.S. Export Administration Regulations (EAR) provide a range of licence exceptions under Part 740, including GBS, TSR, APR and ENC.



geopolitical and international security environment since the recast of the Dual-Use Regulation entered into force has demonstrated the continued relevance of a common EU export control framework. At the same time, it underlines the need for its implementation to remain effective, proportionate, harmonised and closely coordinated with trusted partners, ensuring that evolving security challenges are addressed without creating unnecessary fragmentation or undermining Europe's competitiveness. It should identify opportunities to improve its implementation, strengthen legal certainty and harmonisation across Member States, reduce unnecessary administrative burdens, and ensure that the Regulation continues to support legitimate trade and the competitiveness of companies operating and investing in Europe.

The clarifications provided in the Commission guidelines published in October 2024 and upcoming ITT Commission guidelines should be reflected in the Dual-Use Regulation, ensuring consistent application across the EU. Businesses need legal certainty through clear definitions and consistently applied export licensing criteria.

Export control procedures should remain proportionate and operationally workable. Where risks are effectively controlled, simplified and accelerated procedures should be considered for legitimate service, maintenance and software support.

In general, any evaluation or review of the Dual-Use Regulation should be coordinated with the private sector. The evaluation of the Dual-Use Regulation should ensure coherence with the European Economic Security Strategy and subsequent initiatives, while it is crucial to ensure they do not hinder European competitiveness globally.



FOR MORE INFORMATION, PLEASE CONTACT:

Lourdes Medina Pérez

Senior Manager for International Affairs and Trade Policy

lourdes.medina@digitaleurope.org

Joel Guschker

Associate Director for International Affairs and Trade Policy

joel.guschker@digitaleurope.org

Ludovica Colosimo

Policy Officer for International Affairs and Trade Policy

ludovica.colosimo@digitaleurope.org

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European digitalising businesses across multiple sectors and citizens to prosper from digital technologies. We wish for Europe to grow, attract and sustain the world's best digital talents, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters, and contribute to their development and implementation. Our membership represents over 56,000 businesses who operate and invest in Europe. It includes corporations and scaleups who are global leaders in their field of activity, as well as national trade associations from across more than 30 European countries.