

Towards a Modern Export Control Framework

Executive summary

- The evaluation of the Dual-Use Regulation (EU) 2021/821 should deliver clearer, more harmonised, and predictable implementation across Member States. ESIA calls for greater legal clarity at EU level in the recast of the Dual-Use Regulation, particularly through more precise legal definitions and clearer rules governing software, technology, and other intangible transfers.
- Reducing regulatory fragmentation arising from divergent national controls on non-listed item should be a priority. Moreover, EU-level guidance should complement the legal framework by supporting its consistent interpretation and practical implementation. To remain effective and relevant, such guidance should be regularly reviewed and updated to reflect regulatory developments, technological advances, and practical challenges encountered by industry.
- EU General Export Authorisations (EUGEAs) should be further expanded and harmonised as EU-wide compliance and facilitation tools. ESIA calls for broader use for trusted destinations and intra-group transactions, simplified EU007 reporting, and a new EUGEA for temporary exports, re-exports and transfers of controlled items, software, and technology
- The framework should remain proportionate and responsive to technological developments. ESIA recommends regular review of Article 5 guidance on cyber-surveillance items and proportionate transparency on export patterns and trends of concern, providing greater legal certainty while supporting effective controls.

Introduction

The European Semiconductor Industry Association (ESIA) represents Europe-based leadership in semiconductor research, design, and manufacturing. Semiconductors are essential to Europe's digital and green transitions and underpin key sectors such as automotive, industry, security, healthcare, energy, and communications. The European semiconductor industry operates in a highly global environment and depends on open markets, international cooperation, and clear and predictable rules to remain competitive.

ESIA welcomes the opportunity to contribute to the evaluation of Reg (EU) 821/2021, hereinafter 'the Regulation'.

In the following paragraphs ESIA outlines the main priorities for Europe's the semiconductor sector.

I. Guiding principles: a proportionate and risk-based approach

The Regulation should continue to protect legitimate security and human-rights objectives, but its implementation should more clearly differentiate transactions according to actual risk. In practice, controls can impose disproportionate burdens on recurring lower-risk activities, including intra-group technology collaboration, temporary movements, and routine digital business processes.

Clearer rules, EU-level guidance, harmonised implementation, and well-designed general authorisations would help export controls more effective. They would allow authorities and companies to concentrate compliance resources on transactions that present more meaningful diversion, proliferation, misuse or security concerns. A modern framework should therefore combine strong safeguards for genuinely sensitive transfers with simpler treatment of well-controlled, lower-risk activity.

The EU should ensure that restrictions are targeted at genuinely advanced and choke-point technologies and their related items. The identification of such technologies and related items should be carried out in close consultation with Europe's industry.

II. Harmonisation of national controls

A key objective of the upcoming review of the Regulation must be greater coordination and harmonisation between EU Member States on dual-use export controls, including their practical application. As several semiconductor devices are classified as dual use, a clear legislative framework is paramount for the semiconductor industry. The review should support greater EU-wide convergence, to minimise divergent national interpretations, and preserve a level playing field. Against the backdrop of geopolitical tensions, it increasingly necessary for the EU to speak with one voice on export controls and protect Europe's industry's interests globally.

Several Member States have introduced unilateral national controls to address perceived gaps in the EU control list, including where international export control regimes have not reached consensus on emerging technologies. This has been particularly visible in the semiconductor sector, where additional national measures may cover specific technologies, equipment, software or technical assistance. While such measures may respond to legitimate security concerns, their proliferation has created an increasingly fragmented regulatory landscape across the Union.

Exporters operating in several Member States can no longer rely solely on Annex I of Regulation (EU) 2021/821 to determine their obligations. They must also monitor national control lists and measures that can differ in scope, interpretation, publication method, and update cycles. The same item may therefore be subject a license in one Member State while remaining uncontrolled in another. This reduces legal certainty, increases compliance costs, and risks undermining the Single Market.

A further challenge arises from the interaction between national controls and subsequent updates to Annex I. National measures may later be fully or partly incorporated into the EU control list, creating overlapping or unclear requirements, and increasing the risk of inconsistent implementation and compliance errors.

Series 500 in Annex I should therefore be regularly reviewed and updated to ensure that relevant controls are reflected at EU level and to avoid unnecessary overlaps with national measures.

The Commission's compilations of national measures are useful, but periodic updates cannot function effectively as an operational compliance tool when national rules change between publication cycles. The Commission should therefore establish a centrally managed and continuously updated EU database of national export control measures applicable to non-listed items. The database should be available in several languages, link directly to the relevant national legislation, indicate the entry-into-force date of each measure, and reflect amendments or repeals without delay.

More fundamentally, the Commission should pursue greater EU-level harmonisation of controls on emerging technologies. Member States should retain the ability to introduce temporary measures in response to urgent security concerns, but these should be assessed promptly and, where appropriate, integrated into a common EU framework. This would prevent national controls from becoming a permanent substitute for EU-wide rules, reduce regulatory fragmentation, and strengthen the Single Market while preserving legitimate security objectives.

In the current context of increasing global competition in the semiconductor industry, the EU should further avoid introducing controls that worsen the economic framework conditions for European exporters. The global level playing field should be preserved and improved, and Europe's semiconductor industry should enjoy the same facilitation and advantages that are available to exporters from third countries.

Aiming for closer coordination with like-minded countries, controls should be implemented on a multilateral basis to provide greater consistency and to avoid subjecting industry to restrictions that do not apply to non-EU countries.

III. Establish a permanent EU industry advisory mechanism on export controls

The EU lacks a permanent and structured mechanism for industry and exporters to provide technical input on export controls. In other major jurisdictions, formal consultative bodies allow industry stakeholders and exporters to advise authorities on technical, implementation, and compliance issues. While EU institutions and Member States regularly engage with industry through meetings and consultations, these exchanges are not organised through an equivalent permanent structure. This limits systematic access to industry expertise and reduces the efficiency and predictability of the EU export control system.

ESIA therefore advocates for the establishment of a permanent EU-level industry advisory mechanism on export controls. Such a mechanism should enabling industry and exporters to contribute technical expertise on relevant technologies, supply chains, and the practical implications of existing and proposed controls.

The mechanism should also promote greater transparency on export control decisions at EU level, particularly amendments to Annex I of the Regulation. While updates to the control list are generally published before entering into force, further explanations of the

rationale behind these changes, including the inclusion of specific items or technologies, would help companies better anticipate regulatory developments, assess potential impacts, and adapt their compliance processes accordingly.

A permanent and structured dialogue with industry would also contribute to closer coordination among Member States, more consistent implementation of export controls and a more coherent EU approach towards third countries. This would strengthen the effectiveness and predictability of the EU export control framework while ensuring that legitimate security objectives continue to be met.

IV. Clearer and more modern controls on intangible transactions

One of the most significant weaknesses of the current framework is that the practical application of controls remains better suited to tangible items than to modern intangible transactions and international digital collaboration. Although the Regulation covers software and technology transferred by electronic means, it provides limited guidance on deployment models such as Software-as-a-Service (SaaS), cloud computing, hosted development environments, AI platforms, and collaborative engineering tools.

This creates legal uncertainty about when a digital export occurs, who should be treated as the exporter and how concepts such as “*transmission*”, “*making available*”, and “*access*” should be understood. Divergent national approaches create material compliance challenges. For example, some approaches may treat storage of controlled software or technology on infrastructure outside the EU as an export, while others focus on whether controlled content is actually accessible in readable or usable form to a recipient outside the EU.

The Commission should clarify and harmonise, in the revised Regulation, the concepts of export, transfer, making available, access, and exporter in the digital environment. The rules should adopt a risk-based approach focused on actual access to and usability of controlled software or technology, rather than solely on the technical location of servers or data storage infrastructure.

In particular, the Commission should clarify that the mere storage or processing of encrypted controlled data on infrastructure in a third country should not, by itself, constitute an export where the infrastructure provider cannot access the controlled content. Likewise, access to the functionality of a SaaS product should not automatically be treated as an *export* of the underlying controlled software where the user does not receive or gain access to the software, source code or controlled technology itself. A regularly updated practical EU-level guidance should be issued to ensure that exporters and licensing authorities apply these concepts consistently across Member States.

Greater harmonisation in this area would improve legal certainty, support innovation, and cross-border technical collaboration, reduce unnecessary compliance costs, and make EU export controls more effective in an increasingly digital economy.

Rules for cloud-based processing should reflect modern cloud and AI services

Cloud providers increasingly rely on globally distributed infrastructure and may dynamically change where customer data is stored, transmitted or processed without the customer selecting, controlling or knowing the specific location. The same issue arises with AI and large-language-model services, where technical data may be processed transiently across distributed infrastructure without being permanently stored or made available to the service provider in usable form. Requiring exporters to identify and license every infrastructure location in such circumstances may create significant legal uncertainty and administrative burden without necessarily corresponding to an increase in export control risk.

The regulatory assessment should focus on whether controlled software or technology is actually accessible in intelligible or usable form to an unauthorised person outside the EU. Risks should be managed through safeguards such as encryption, technical access controls, authentication, user authorisation, and appropriate contractual and organisational measures, rather than requirements to “claw back” technology after access or processing where this is not technically feasible.

V. Cyber-surveillance items: clearer guidance, transparency and trend information

The treatment of cyber-surveillance items under Article 5 requires particular attention because relevant technologies can be widely used for legitimate commercial purposes and can be difficult to manage in practice. Clear, regularly updated EU-level guidance is essential to ensure that exporters and authorities apply the rules consistently and can distinguish higher-risk uses from ordinary commercial activity.

The Commission should regularly review and update the guidelines on the export of cyber-surveillance items under Article 5, taking account of technological developments and implementation experience across Member States. Guidance should be sufficiently practical to support classification, due diligence, and end-use assessment without creating unnecessary uncertainty for commonly used technologies.

Transparency should also be improved in a proportionate manner. The Commission should publish more detailed aggregated information on exports of cyber-surveillance items and should more actively communicate trends of concern, such as unusual changes in export patterns to particular regions or material shifts in trade following the introduction of restrictive measures. Such information can help companies improve risk screening and can support more consistent enforcement, while appropriate safeguards should continue to protect commercially sensitive and security-sensitive information.

VI. Expansion, simplification and harmonisation of Union General Export Authorisations

Expand simplified authorisations for low-risk intangible transfers

The Commission should consider introducing appropriately designed licence exceptions or expanding EU General Export Authorisations (EUGEAs) to cover recurring low-risk intangible transfers, subject to appropriate safeguards. This would reduce administrative burdens for exporters and competent authorities while allowing licensing resources to focus on higher-risk transactions.

Expand simplified authorisations for trusted destinations

The Regulation provides simplified licensing mechanisms that facilitate exports to trusted partner countries with robust export control systems. However, some strategically important jurisdictions are not covered by existing simplified mechanisms despite being key technology partners, maintaining strong export control frameworks and playing important roles in global high-technology supply chains. Exports to these destinations may require individual licences, adding administrative burden, cost, and delay without necessarily producing a corresponding security benefit.

The Commission should assess whether existing EUGEAs can be expanded to additional trusted destinations that maintain equivalent export control standards and are closely integrated into global technology supply chains. It should also examine national general export authorisations used by Member States and consider whether effective national models should be incorporated into existing EUGEAs or used as the basis for new EU-wide authorisations.

Harmonise EUGEA implementation across Member States

The benefits of EUGEAs are reduced when national implementation practices differ significantly. Reporting obligations, reporting frequency, required data fields, notification requirements, and submission methods should therefore be harmonised as far as possible across Member States.

Greater reliance on harmonised EU authorisations would improve consistency across the Single Market, reduce regulatory fragmentation, and allow competent authorities and industry to devote resources to transactions with greater diversion, proliferation or security risk.

Modernise EUGEA for intra-group transfers: Broader scope and proportionate reporting

The EUGEA for intra-group transfers (EU007) should be further developed to better reflect how multinational companies develop, maintain, and support technology. Controlled software and technology are frequently exchanged across group entities for engineering, R&D, cybersecurity, product support, and other collaborative activities.

The Commission should assess whether EU007 could be expanded to cover a broader range of intra-group relationships and destinations, provided that effective corporate control and appropriate safeguards remain in place. These should include an Internal

Compliance Programme (ICP), access controls, screening, due diligence, risk assessment, and record-keeping.

ESIA also believes that the periodic reporting requirement under EU007 should be removed. EU007 already applies within closely controlled corporate structures and is subject to material safeguards, including an ICP, registration with the competent authority and notification of first use. Given the frequency with which controlled software and technology may be accessed or exchanged within multinational groups as part of routine business and technical activities, periodic transaction reporting can create significant administrative burdens for both exporters and competent authorities without commensurate additional security value where transfers remain within a defined corporate group and are governed by effective compliance, due diligence, and risk management controls.

Mandatory periodic reporting should be replaced by a proportionate record-keeping obligation. Exporters should maintain sufficient information on transfers and make relevant records available to the competent authority upon request. Competent authorities should retain audit and supervisory powers, while registration, first-use notification, and other proportionate safeguards remain in place. This would preserve traceability and effective oversight while directing supervisory resources towards higher-risk transactions rather than routine intra-group activity.

Member States should not be able to reintroduce equivalent routine reporting obligations through national implementation, as this would undermine the administrative simplification intended by an EU general authorisation. EU007 should provide the same core level of administrative simplification and regulatory predictability across regardless the Member States in which the exporters are established.

Modernise EU007 for technology retention and use

The requirement to return exported software and technology to the exporter and completely delete it at the end of the relevant development activity does not reflect the way technology is developed and managed in modern industrial groups. Technology is typically retained, maintained and further developed throughout the product life cycle, including engineering, cybersecurity, maintenance, and product support.

EU007 should instead permit continued retention and use within the authorised corporate group, subject to effective access controls, an appropriate Internal Compliance Programme and compliance with the authorisation. Where an entity ceases to be eligible under EU007, access should be terminated and the technology deleted or its continued retention covered by another appropriate authorisation.

Adapt EU007 for modern intra-group ownership structures

EU007 should not be limited to directly owned subsidiaries and sister companies, but should be capable of covering indirect subsidiaries and other entities under common ultimate ownership or control, including groups operating through several levels of holding companies, provided that effective group control and appropriate compliance safeguards are demonstrated. Similarly, the destination scope should be reviewed on a risk-based basis, with broader coverage of jurisdictions presenting an appropriate export control and security risk profile, and appropriate exclusions for sensitive destinations, end-users, and end-uses. EU007 should also expressly accommodate access to controlled software and

technology by employees who are temporarily travelling or working remotely from an eligible third country, provided that the employee remains subject to the exporting group's employment, compliance, and access control framework, and that applicable destination and end-use restrictions are respected.

Promote reciprocal recognition and coordinated licensing for intra-group transfers

The reciprocal recognition arrangements or coordinated licensing mechanisms with like-minded third countries should be explored by the Commission, to avoid duplicative licensing requirements for intra-group transfers. Such arrangements should enable companies operating under centralised compliance frameworks to benefit from mutually recognised authorisations. This would reduce administrative burdens, improve legal certainty and facilitate international R&D and technology collaboration.

Introduce a new EUGEA for temporary exports

ESIA calls for the introduction of a new EUGEA covering temporary exports, re-exports, and transfers of controlled products, software, and technology. European companies routinely need to move controlled items temporarily for demonstrations and exhibitions, testing and evaluation, servicing, maintenance and repair, employee business travel, customer or employee training, commissioning and installation, and short-term engineering or project deployments.

Individual licensing for these activities can create significant administrative work and delay even where the item is not being sold or permanently transferred, remains under the exporter's ownership or effective control, and is returned after the relevant activity. These cases generally present a different risk profile from permanent transfers to independent third parties and are well suited to a general authorisation with clearly defined safeguards.

Suggested conditions for a temporary-export EUGEA:

- the export is genuinely temporary and undertaken for a defined eligible purpose;
- the exporter retains ownership or effective control of the item, software or technology, as appropriate to the transaction;
- the controlled item is returned to the EU, or otherwise lawfully disposed of or transferred under an appropriate authorisation, within a defined period;
- the authorisation is unavailable where the exporter knows that the item is intended to remain permanently outside the EU or is intended for an unauthorised end-user or end-use;
- appropriate destination, end-user, and end-use restrictions continue to apply;
- controlled software and technology are protected against unauthorised access;
- exporters maintain appropriate records demonstrating compliance with the conditions of the authorisation; and
- particularly sensitive items, destinations or end-uses may be excluded where justified by the relevant security or proliferation risk.

A useful reference model is License Exception TMP under the U.S. Export Administration Regulations (15 C.F.R. § 740.9), which provides for a range of temporary exports, re-exports, and transfers, including tools of trade, exhibitions and demonstrations, inspection, testing and repair, and certain technology used by employees travelling or temporarily assigned abroad. An EU mechanism should be tailored to Regulation (EU) 2021/821 rather than simply replicating the U.S. rules, but the model demonstrates that temporary movements can be managed through a general authorisation with effective-control, access and return/disposition safeguards.

A temporary-export EUGEA would be especially valuable in a digital and internationally collaborative economy. Temporary access to controlled software and technology may arise during employee travel, technical support, cloud-based engineering, testing, and multinational project work just as temporary movements of physical equipment arise during exhibitions, demonstrations, and servicing activities.

Conclusion

The review of Regulation (EU) 2021/821 is an opportunity to make the EU export control framework more coherent, predictable, and better adapted to technological and business realities. Greater harmonisation across Member States and structured consultation with industry are essential to a stronger and more effective EU approach.

At the same time, the framework must keep pace with digitalisation and new ways of developing and sharing technology. Clearer rules for intangible transfers, cloud-based processing, and cyber-surveillance are needed to provide legal certainty while keeping controls focused on genuine security risks.

Finally, the EU should make greater use of harmonised and proportionate facilitation tools. Modernised and expanded EUGEAs, simpler requirements for the intra-group transfers EUGEA, as well as a new EUGEA for temporary exports, re-exports, and transfers can reduce unnecessary administrative burden and allow both authorities and industry to focus resources where security risks are greatest.

Summary

Area	Key proposals	Expected benefits
1. Risk-based approach to export controls	Apply more proportionate controls based on actual risks. Focus restrictions on genuinely advanced and critical technologies, identified in consultation with industry.	Reduce unnecessary compliance burdens while maintaining security safeguards.
2. Harmonisation of national export controls	Strengthen EU-wide coordination; create a continuously updated EU database of national controls; regularly review Series 500 in Annex I; prioritise common EU rules over divergent national measures.	Improve legal certainty, reduce fragmentation and preserve the EU Single Market.
3. International coordination	Promote multilateral export controls and closer alignment with like-minded countries. Avoid unilateral restrictions that disadvantage European exporters.	Maintain a global level playing field and strengthen EU competitiveness.
4. Permanent industry advisory mechanism	Establish a formal EU-level platform for industry consultation on export controls, technical developments, and Annex I amendments. Improve transparency regarding regulatory decisions.	Ensure industry expertise informs policy and increase predictability.
5. Intangible technology transfers	Clarify the concepts of export, transfer, access, and exporter in digital environments. Develop harmonised guidance for SaaS, cloud computing, AI platforms, and digital collaboration.	Reduce uncertainty and facilitate international R&D and technology collaboration.
6. Cloud and AI services	Focus export control assessments on actual access to controlled technology rather than server location. Clarify treatment of encrypted data and cloud-based processing.	Enable modern digital business operations without unnecessary licensing burdens.

7. Cyber-surveillance items	Regularly update Article 5 guidance and publish more aggregated export data and information on concerning trade trends.	Improve due diligence, risk assessment, and consistent application of controls.
8. Expansion of EU General Export Authorisations (EUGEAs)	Extend existing EUGEAs to additional trusted destinations and consider incorporating effective national authorisation models into EU-wide mechanisms.	Simplify exports to trusted partners and reduce licensing delays.
9. New EUGEA for temporary exports	Introduce a general authorisation covering temporary exports for exhibitions, testing, repairs, training, employee travel, and short-term technical projects, subject to appropriate safeguards.	Reduce individual licensing requirements for lower-risk temporary activities.
10. Harmonisation of EUGEA implementation	Standardise national reporting obligations, notification procedures, required information, and submission methods.	Ensure consistent implementation and administrative simplification across the EU.
11. Modernisation of EU007	Expand EU007 to cover more intra-group relationships, indirect subsidiaries, destinations, and temporary remote access by employees. Remove periodic transaction reporting and replace it with proportionate record-keeping and disclosure upon request. Prevent Member States from reintroducing equivalent obligations. Allow controlled technology to remain within authorised corporate groups throughout its lifecycle, subject to safeguards, rather than requiring automatic deletion after development activities. Explore reciprocal recognition arrangements or coordinated licensing mechanisms with like-minded third countries.	Facilitate international R&D and technology collaboration, reduce administrative burdens and duplicative licensing requirements, and improve legal certainty for multinational companies.

For further information:

Giovanni Corder

Deputy Director General, Senior Director Global Policy

European Semiconductor Industry Association (ESIA)

Tel: + 32 2 290 36 60 • Web: <https://www.eusemiconductors.eu/esia>

ABOUT ESIA

The European Semiconductor Industry Association (ESIA) is the voice of the semiconductor industry in Europe. Its mission is to represent and promote the common interests of the Europe-based semiconductor industry towards the European institutions and stakeholders in order to ensure a sustainable business environment and foster its global competitiveness. As a provider of key enabling technologies, the industry creates innovative solutions for industrial development, contributing to economic growth and responding to major societal challenges. Being ranked as one of the most R&D-intensive sectors by the European Commission, the European semiconductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 jobs indirectly in systems, applications and services in Europe. Overall, micro- and nano-electronics enable the generation of at least 10% of GDP in Europe and the world.