AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Export controls in the context of cloud computing (January 2025)

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive Summary

On 29 October 2021, the American Chamber of Commerce to the EU (AmCham EU) published a position paper highlighting the need for clearer guidance on the application of export controls under Regulation (EU) 2021/821, (the 'Dual-Use Regulation'), focusing on the use and provision of cloud computing services. Ahead of the evaluation of the Dual-Use Regulation, AmCham EU again urges the European Commission to clarify how export controls apply in the context of cloud computing. The most critical issues for attention include 1) what constitutes an 'export' in the context of dual-use software and technology stored in the cloud, 2) who the 'exporter' is in these cases and 3) what activities are not exports under certain conditions. Further clarification on these issues is essential to achieve a harmonised application of export controls within the EU.

Harmonisation is needed at EU level and globally

Clarifying the application of the Dual-Use Regulation to cloud computing services will significantly contribute to the EU's objectives in the field of export controls. As noted by the Commission in its White Paper on Export Controls, published in 2024, there is a 'need for more rapid and coordinated action at EU level in the area of export controls', 'where divergences between Member States would weaken the economic security of the EU as a whole'.[1] The Dual-Use Regulation is silent with respect to its application to cloud computing services, which has resulted in divergent interpretations between Member States and with multilateral partners, such as the United States and United Kingdom. Providing additional guidance in this area at EU level will contribute to the EU's primary objective of achieving a high level of harmonisation.

Businesses require clear and consistent rules globally. Managing divergent regulatory requirements and processes adds complexity and administrative burdens, reduces business agility and hinders competitiveness. EU industry would benefit from a clear and harmonised approach to cloud computing services and intangible technology transfers within Europe as well as alignment between the EU and other like-minded countries. Through the publication of its own guidance[2], the UK has already taken steps towards clarifying key aspects of software and technology transfers via the cloud, aligning with the interpretations and approaches of the U.S. To that end, the Commission should also aim to introduce guidelines for Member States that will:

- Ensure protection of international security and equal opportunities for all.
- Provide clarity on what constitutes an 'export' when intangible items are transferred via IT providers, such as cloud computing.
- Simplify compliance with export controls by standardising processes across regions.
- Put exporters in Europe on equal footing and promote simplified trade between trading partners.
- Offer greater flexibility to exporters and reduce the disparity of administrative burden between EU and US exporters.

In addition, a centralised position at EU level will increase transparency and provide businesses with the clarity required to take full advantage of cloud computing services.

[1] European Commission, White Paper on Export Controls, 24.1.2024.

[2] https://www.gov.uk/government/publications/exporting-military-or-dual-use-technology-definitions/export-of-technology-remote-access-and-the-use-of-cloud-computing-services

Key recommendations

To address the current lack of clarity, the following four principles should govern the application of the Dual-Use Regulation in the field of cloud computing services. These basic principles should serve as guiding tenets in the context of access to dual-use software and technology via cloud services utilising data centers and servers across borders.

1. Providing access to cloud services, including Software as a Service (SaaS), is not an 'export'

Article 2(2)(d) of the Dual Use Regulation determines that an 'export' depends on whether there is 'transmission'. In contrast, to download or install, the access to software via a data center or server located within the EU does not amount to transmission because the user is unable to access the underlying code that gives the software its controlled character. Therefore, this scenario does not entail any transmission or export. Where a person or user outside the EU electronically accesses commercial computing hardware in the EU via the internet for the storage of data (in the context of infrastructure as a service), the actual hardware (i.e., servers) are not exported or transmitted to the user and thus there is no export of a dual-use item.

Proposed guidance:

Under Article 2(2)(d) of the Dual-Use Regulation, the key element to determine whether an 'export' of software or technology takes place is to identify whether dual-use software or technology has been 'transmitted' to a person outside the EU. Whether a transmission has occurred depends on the nature of the item being transmitted and the type of access granted.

'Transmission' typically occurs when software is sent via email, file-sharing services, physical storage devices, or when it is made available for download, providing access to the underlying code (object code or source code) that makes the software executable or viewable. In contrast, software as a service (SaaS) arrangements merely provide functional access to software without enabling the recipient to download or view the underlying code, thereby preventing any tangible transmission or export of controlled software or technology.

Uploading dual-use software or technology to the cloud does not, in itself, constitute an export – regardless of the location of the server. An export occurs only when:

- The use of cloud storage located outside the EU for storage of dual-use software or technology is downloaded and fully executable in unencrypted form to a recipient outside the EU.
- Controlled items uploaded to the cloud are downloaded or accessed by persons located outside of the EU.

If stored items remain accessible only to persons within the EU, no export takes place, even if the computing hardware (i.e., servers) is located abroad. Encryption plays a crucial role: if the software or technology is encrypted in a way that prevents unauthorised decryption, no export occurs.

Where a person or user located outside of the EU accesses the functionality of software through the cloud and such access does not require a download or local installation (i.e., SaaS), there is no transmission of the software to that person outside the EU and therefore there is no export of that software. Access to technology or source code is considered an export only when:

- The person or user outside the EU receives the underlying code (i.e., object code or source code) in an unencrypted form. Access to technology or source code occurs when the user actually views the technology or source code in an unencrypted form.
- The person or user outside the EU accesses the object code by downloading it in an unencrypted form.

In the case where the technology or software is secured using encryption that the recipient cannot remove, it is not viewable (in the case of technology or source code) or executable (in the case of object code) and hence not exported. Accordingly, in the cases where the technology or software is not encrypted, there can be access to the software or technology outside the EU, and an export can occur.

2. Cloud users are the 'exporter' of their controlled goods, not the cloud service provider

Article 2(3)(b) of the Dual-Use Regulation states that the exporter is the person who decides to transmit or make available software and technology outside the EU. In the context of cloud services, the cloud user determines whether to transmit or make available their software or technology. The cloud service provider does not have control or knowledge of where, when and to whom its users are transmitting data. Therefore, the 'exporter' is the cloud user.

Proposed guidance:

When users of a cloud service transmit, store, process or otherwise use controlled technology in a way that causes an export, it is the cloud user – not the cloud provider – that is the exporter.

Under Article 2(3)(b) of the Dual-Use Regulation, the 'exporter' in the context of cloud computing services is the cloud user, as the cloud user decides whether their software or technology in the cloud can be downloaded or, in the case of source code or technology, viewed by persons outside the EU. The cloud service provider generally does not have information about whether the cloud user's content is export controlled, nor does the cloud service provider determine where, when and to whom its users are transmitting data. There may be certain scenarios where a cloud service provider is using the cloud to export its own controlled items, in which case the cloud service provider would also be the cloud user and, as such, the exporter.

When providing access to controlled technology or software, the exporter is the party that controls and provides the right to access information (e.g., access control lists, decryption keys, network access codes or passwords) so that the controlled content can be fully accessed outside the EU. As such, the jurisdiction of the exporter's location should determine the applicable export control rules. For example, if an EU-based cloud user provides access to controlled software for a person outside the EU, the cloud user is responsible for ensuring compliance with EU export controls, irrespective of where the cloud service provider's data centers are located.

3. Encrypted data is not 'exported' until it is (a) transmitted, (b) decrypted, and (c) actually accessed by the recipient

Uploading dual-use software or technology to a server outside the EU or using a server in the EU from outside the EU should not constitute an 'export', as long as the software or technology is adequately protected from access. Encryption ensures that the controlled content remains inaccessible, indecipherable and unusable until decrypted, thereby preventing its export until specific conditions are met.

When controlled technology is encrypted according to industry standards, the controlled content is not accessible before decryption. Encrypted technology is indecipherable and unusable. It cannot be accessed by users, and there is no risk of diversion of the underlying technology. Therefore, the use of a server in the EU by a person located outside the EU is not an export, provided that the controlled software/technology is adequately protected from access, for example by applying industry standard encryption which makes access to it technically impossible. Similarly, uploading encrypted software/technology to a server outside the EU does not constitute an 'export' because the controlled content remains inaccessible without decryption.

Proposed guidance:

Dual-use technology that is encrypted and stored on (or transiting) a server outside the EU does not require an export authorisation. By applying end-to-end encryption to the controlled technology, the controlled technology itself has not been exported. Only a series of uncontrolled alphanumeric characters that are non-arbitrary (i.e.,

the encrypted content) have been transmitted. Therefore, an export of end-to-end encrypted software/technology will only occur when the means to access the controlled software or technology (i.e., decryption key or password) is made available to the recipient. Should an export occur, the export will be considered from the EU to the location of the person accessing the decrypted software or technology. For example, if an employee in the EU sends encrypted technology to a person in India and subsequently provides the decryption key, an export authorisation may be required for an export to India.

To prevent unintended exports of dual-use software or technology stored in the cloud to persons outside the EU, users of cloud services for storage, processing and use of dual-use software and technology in the EU can make use of appropriate IT safeguards, such as industry-standard methods of end-to-end encryption (e.g., ISO/IEC 19790). Where such means are used effectively, the controlled content of the software or technology would be unusable to another person without the means to decrypt it. In summary, export authorisation requirements should be based on the location of the entity providing the decryption key (exporter) and the location of the recipient accessing the decrypted content (importer), rather than the physical location of the server where the encrypted content is stored.

4. The use of IT or administrative support personnel located outside the EU for cloud workloads does not give rise to an 'export'

When the dual-use software/technology is adequately protected, for example by means of encryption, access to it is technically impossible. Even if it is not encrypted, IT or administrative support personnel generally do not have actual access to the controlled software or technology. Therefore, an export authorisation should only be required when the user believes IT personnel may need to actually access the controlled software or technology in unencrypted or viewable form.

Proposed Guidance:

The presence of IT or administrative support personnel outside the EU, whether employed by the cloud user or the cloud service provider, does not result in an export if the dual-use software or technology is encrypted. Encryption ensures that the controlled software or technology remains inaccessible and unusable, preventing any risk of unauthorised access.

Even if the software or technology is not encrypted, such IT support personnel generally do not have actual access to the controlled software or technology, as there are usually processes to segregate controlled workloads from the general IT support tasks. Consequently, no export would occur and no authorisation would be required.

However, in cases where the user believes IT support personnel outside the EU may need to access controlled items in unencrypted or viewable form, then an authorisation would be required prior to such access. Users should put measures in place to prevent access to controlled items to IT and administrative support personnel. However, if an export takes place, the party in the EU making the controlled item available (i.e., the user of the cloud services) would be the exporter.

Conclusion

The absence of clear and precise rules governing the application of the Dual-Use Regulation in the field of cloud computing services risks creating different interpretations and significant divergences across Member States. This not only harms the EU's efforts to achieve harmonisation but also risks depriving the EU as a whole from the benefits associated with such services, including enhanced security, encryption at rest and in transit, cost efficiency and access to cutting-edge technology, particularly AI and machine learning capabilities which can assist in compliance monitoring by flagging potential export control violations.

AmCham EU encourages the Commission to develop detailed guidance in line with the above recommendations.