DIGITALEUROPE

8 July 2021

Export Controls Tech Transfers

Introduction

The European Union's ("EU") definition of "export" is ambiguous as it relates to intangible transfers of software and technology.[1] This ambiguity creates differing interpretations and regulatory requirements for intangible transfers within the EU and between the EU and its global allies. It also creates unnecessary complexity and costs for exporters in the EU, putting them at a competitive disadvantage.

In accordance with recital 11 of the EU Dual Use Recast ("Recast"), DIGITALEUROPE understands that the EU Commission ("Commission") is considering guidelines that will provide "harmonised interpretations of provisions" for intangible exports and "limit the administrative burden for exporters and the competent authorities of the Member States."[2] DIGITALEUROPE welcomes these guidelines as an opportunity to achieve what the Recast sets out to do, while ensuring the security and competitiveness of Europe's digital economy. We present below five key recommendations for the Commission to consider while formulating these guidelines.

Background and Need for Guidelines

The Netherlands, Germany, the United Kingdom, and the United States have all published guidance or regulations that take different approaches and apply different standards to various aspects and types of intangible transfers. This lack of alignment increases the complexity faced by EU exporters, increases hesitancy to embrace digital transformation, and ultimately harms the competitiveness of EU business.

At a time when Europe is entering the "Digital Decade" there is a genuine need to modernize and harmonize the application of export controls to intangible transfers. DIGITALEUROPE believes that, through the publication of EU guidelines, the Commission has an opportunity to adopt a pragmatic approach to intangible exports to provide clarity and consistency, reduce administrative burdens, and put EU

[1] "Export means . . . transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the customs territory of the Union; it includes making available in an electronic form such software and technology to natural or legal persons or to partnerships outside the customs territory of the Union; it also includes the oral transmission of technology when the technology is described over a voice transmission medium." *European Parliament legislative resolution of 25 March 2021 on 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), Article 2, Part 2(d).*

[2] *European Parliament legislative resolution, 25 March 2021; Recital 11.*

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

exporters onto a level playing field with their global counterparts, all without compromising the ultimate objectives of export controls. Anything less than this will result in damage to the EU's high-technology companies as they are forced to devote resources to managing disparate rules at the member state, EU, and international levels.

DIGITALEUROPE Recommendations

DIGITALEUROPE suggests that EU guidelines on intangible transfers adopt the following positions:

1. Encrypted technology is only exported at the time of decryption and access

The EU guidelines should confirm that no "export" occurs when *encrypted* technology is sent outside of the EU unless and until the technology is also decrypted and accessed outside of the EU.

When controlled technology is encrypted, the technical 'know-how' that is the reason for control is not "made available" to anyone until the technology is decrypted. Encrypted technology is indecipherable, unusable, and robust – encrypted technology cannot be viewed or applied to an end-use until it is decrypted, and there is no possibility of diversion of the underlying technology. This is the reason that, e.g., US regulators exclude encrypted data transfers from the definition of "export" under US military/defence controls.

This position is also consistent with the Recast definition of "export" and would reduce unnecessary administrative burden for both exporters and export control authorities (e.g., because no export licenses would be required for technology that may be sent or stored but never decrypted outside the EU). Additionally, this position incentivizes and encourages the use of encryption, which will lead to increased data security for industry, governments, and individuals.

There are many ways that the Commission and member states could tailor this position to address any potential concerns. For example, the United States has adopted this position for both military technical data (under the International Traffic in Arms Regulations (ITAR), as mentioned above) and dual-use technology (under the Export Administration Regulations (EAR)). Both the EAR and the ITAR include certain conditions on the applicability of this position, requiring, for example, that the encryption used is compliant with specific and recognized security standard (e.g., at least 128 bits of security strength) and that the encrypted technology not be sent to or stored in certain countries of concern.[3]

In sum, adopting this position for encrypted technology will increase data security, reduce unnecessary administrative burdens, and put EU exporters on an equal footing with US exporters.

[3] US International Traffic in Arms Regulations, 22 CFR §120.54; US Export Administration Regulations, 15 CFR §734.18.

2. There is no export of Software in the Software as a Service (SaaS) model

The EU guidelines should explicitly recognize that software is not "exported" when the software is provided as a service because no software is transmitted to or downloaded by the user.

Software as a service (Saas) generally involves hosting software in one location and allowing that software to be used from other locations via the internet. SaaS does not require the party hosting the software to transmit the software (i.e., the underlying code) to users, nor does it require users to download the software. Therefore, there is no risk of unauthorized proliferation of the underlying code. EU guidelines on intangible transfers should recognize that SaaS does not involve download or other receipt of software for users. Therefore, providing SaaS is not an "export" of a dual-use item.

For comparison, the United States has adopted this position in a series of advisory opinions published between 2009 and 2014,[4] and the UK takes a similar position in a case study included in its recently-published guidance on "Exporting military or dual-use technology: definitions and scope" ("UK Guidance").[5] EU adoption of the rule would level the playing field for EU exporters and reduce the complexity caused by treating SaaS differently in different countries inside and outside the EU.

---

[4] Application of EAR to Grid and Cloud Computing Services, 1.13.2009; Cloud Computing and Deemed Exports, 1.11.2011; Cloud-based Storefronts, 11.24.14

[5] The UK Guidance includes this case study: "Company H makes export controlled CAD software for development of active flight control systems available on its intranet as a service. **Access to use the controlled software would not be subject to licensing.** However, accessing or downloading the resultant data overseas may be subject to export licences if the data contains controlled technology" (emphasis added). 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.

3. Administrative Access is not an "export"

EU guidelines should recognize that no "export" occurs when administrators (e.g., at a telecom, cloud service, or SaaS provider) have access to user data for purposes of providing, supporting, or maintaining the service as long as certain safeguards are observed.

The UK Guidance includes a useful case study to this effect:

> **Company J** is a cloud service provider. **Company K** stores controlled technology on **Company J** servers located in the UK or elsewhere. **Company K** has protected the controlled technology stored in the cloud from unintended access, for example by using industry standard encryption, identity and access management or other safeguards. To provide, support and maintain the cloud services, some **Company J** technical, administrative and maintenance personnel are located outside the UK. **Company K** may require **Company J** personnel to manage technical issues in **Company K's** cloud environment. No export licence is required because **Company J** personnel are not the intended recipients of the controlled technology.

By adopting a similar guideline, the EU would again be able to reduce administrative burdens for exporters, service providers, and regulators by reducing the need for export authorizations where a service provider does not need and will not access the substance of a service user's data.

4. Clarification on the responsible Exporter

The Recast defines an "exporter," in relevant part, as "any natural or legal person or (...) partnership that *decides to transmit* software or technology by electronic media, including by fax, telephone, electronic mail or by any other electronic means to a destination outside the [EU] or to make available in an electronic form such software and technology to natural or legal persons or to partnerships outside the [EU]" (emphasis added).[6] Consistent with this definition, the Commission's guidelines should explicitly specify who the exporter is in different scenarios, e.g.:

- As we noted above, providing SaaS is not an "export," so there is no "exporter" in a SaaS scenario.
- When users of a service, transmit, store, process, or otherwise use controlled technology in a way that causes an "export," it is the service user, not the service provider, that is the exporter.

[6] *European Parliament legislative resolution, 25 March 2021; Article 2, Part 3(b).*

- Similarly, when providing *access* to controlled technology the exporter is the party that controls and provides the access information (e.g., decryption keys, network access codes, or passwords) so that, e.g., controlled technology can be accessed outside the EU.

Service providers have no visibility or control over, e.g., when or whether users of a service access, transmit, store, or otherwise use controlled technology. Therefore, service providers have no control over whether users "export" controlled technology when using a service, or when users provide access information such as a password so that controlled technology becomes accessible. For these reasons, the Guidelines should explicitly state that service providers are not the exporters of their users' data or related access information. This position is consistent with the interpretation of "exporter" given in guidance or regulations published by export authorities in the Netherlands, Germany, the UK, and the United States.

5. Industry Input is vital

The intangible technology transfer landscape is complex and continuously evolving. For the sake of brevity, this paper is focused on the headline issues raised by our members. In order to ensure that the Commission's guidelines can effectively address the issues of today and be relevant to the digital Europe of tomorrow, input and consultation from industry will be hugely important. The development of ICP guidelines is a good example of how collaboration between industry and regulators can result in pragmatic and effective results. DIGITALEUROPE stand ready to support the Commission in the development of intangible export guidelines.

FOR MORE INFORMATION, PLEASE CONTACT:

Tsai-wei Chao-Muller

Policy Director, Digital Technology, Innovation and Trade

Tsai-wei.Chao@digitaleurope.org

Joël Guschker

Policy Officer, Trade and International Affairs

joel.guschker@digitaleurope.org

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK