Proposal for Recast of Export Control Regulation: DIGITALEUROPE Comments on Council Negotiations

Brussels, 11 July 2018

Introduction

DIGITALEUROPE, the industry association representing the digital technology industry in Europe, has been closely following the negotiations in the European Parliament and the Council on the European Commission's proposal for a reform of the EU Export Control Regime. DIGITALEUROPE fully endorses the need to address the latest technological and political developments but harbours concerns with regard to specific amendments further outlined below. Taking stock of the efforts of the co-legislators to enhance the European Commission's proposal, DIGITALEUROPE would like to contribute with the ICT industry's perspective to the ongoing discussions in the Council working party for export control. Thereby, we seek to ensure that businesses can fully benefit from the reform in practice.

In the following, we set out our view on the proposals for:

1. EUGEA No. EU009 on Encryption
2. EUGEA No. EU008 on Intra-company Transmission of Software and Technology Transfers
3. EUGEA No. EU003 Export after Repair/Replacement
4. New Catch-all Controls
5. Autonomous List

1. EUGEA No. EU009 on Encryption

Starting out as a specialized tool for protecting the confidentiality of sensitive human communication, cryptography is now an omnipresent enabler of security for connected infrastructure and appliances as well as the cornerstone of personal integrity and accountability on the Internet (see DIGITALEUROPE explanatory video here). DIGITALEUROPE supports the steps taken by the European Commission to reduce the barriers surrounding the handling of this crucial technology. At the same time, we are sympathetic to the dual-edge nature of encryption in certain applications and understand why certain government insight may still be relevant, for instance for purposes of combating terrorism and organized crime.

ICT is today a software-dominated business where agile deployment with short release-cycles is expected to remain competitive. In such an environment, any additional step of track-keeping or evaluation of a product in relation to given criteria drives significant costs, not only directly through requirements on IT implementations and/or manual administration, but also through the loss of operational flexibility by adding steps and lead times to the product release flow. Harmonization of EU export controls with other states, particularly the US, is therefore paramount for EU companies to have a level-playing field with non-EU companies. We welcome the proposal of new EUGEAs for encryption, which provide similar functions as currently available for encryption under the US export control regulation. However, we would like to outline some important differences that are needed to be addressed in order to ensure a level-playing field.

The European Commission's proposal for EUGEA EU009 differs from the US regulation provisions concerning encryption in that it relies solely on ECCN classification for defining the scope of covered products. This is generally appreciated since it avoids an additional step of classification over the ECCN.

2. EUGEA No. EU008 Intra-company Transmission of Software and Technology Transfers

DIGITALEUROPE welcomes the proposal by the European Commission to establish a new EUGEA on intra-company transmission of software and technology transfers and the respective amendments made by the European Parliament. For the member companies of DIGITALEUROPE, the ability to innovate and offer market-leading solutions and products is closely linked to the free flow of information and technology within a company. To date, these transactions may need multiple export licences from different export authorities for company internal operations. With an effective general licence in place, resources of the private sector and licensing authorities would be saved, and more focus can be given to critical transactions.

DIGITALEUROPE is of the opinion that transfers between corporate entities represent low risk transactions as they will remain within one corporate structure and no external transfer will take place outside the company.

As a further guarantee, the EUGEA proposal also requires that companies must establish an Export Management and Compliance Program (ICP) to ensure consistent instruction and operational application of a company's export policies, procedures, decisions, and transactions. The EUGEA for intra-company transfer of technology and software should therefore cover all internal transfers as long as the technology/software remains under the ultimate ownership of the company – with the possibility to exclude critical countries such as sanctioned countries.

In order to make EUGEA EU 008 effective and ensure an added value for the industry in using it, it is important that it does not only cover transfers from a parent company to its wholly-owned or controlled entities (downstream), but also from a subsidiary / controlled entity back to its parent company (upstream) as well as among its subsidiaries (horizontal transfers). Moreover, the scope of the EUGEA should not be limited to commercial product development but company-internal cooperation projects in general.

An effective and comprehensive EUGEA on intra-company technology transfers would add substantive value to the industry and contribute to reducing administrative burden and speeding up internal processes for instance in the area of product development. As a general rule, global licences do not fulfil these objectives to the same extent as they are too static for an international (project) environment that constantly evolves.

In addition to the intra-company sharing of technology and software, it should also be considered how the transfer of hardware within one corporate structure for research purposes could be facilitated. The European Commission's proposal is limited to software and technology and contains a requirement to list each transferred product with description, ECCN and quantity. Software development according to current industry standards rely on individual developers' down- and uploading pieces of code towards a common code repository, possibly several times per day. Producing an itemized list of each such transmission with ECCN and description would not only be costly, but the resulting report would consist of potentially millions of items, the quantity and description of which would not be apparently usable by an authority. DIGITALEUROPE would therefore prefer that the EUGEA EU008 would not include such reporting requirements.

3. EUGEA No. EU003 Export after Repair/Replacement

As regards the EUGEA for export after repair/replacement, this is a potentially important simplification tool. Many DIGITALEUROPE member companies repair and reuse products and spare parts to extend the lifecycle of products, to support legacy systems and to save energy and use natural resources efficiently. Unfortunately, the ability to use this EUGEA is today limited as it has not kept up to date with the kind of advanced services and circular economy models that many globally leading ICT providers implement. DIGITALEUROPE therefore urges the EU Member States to use the reform of the Export Control Regulation to also modernise the EUGEA EU 003 for export after repair/replacement.

There are two main barriers in the current EUGEA EU003: firstly, that the exported repaired spare part is the same part that was sent to Europe for repair and secondly, that it cannot be used when shipped to a customs-free zone or a free warehouse. As regards the first barrier, this is against advanced services models where DIGITALEUROPE members have service contracts for replacement as low as 2-48 hours. For such services models, spare parts will be held in a number of local depots throughout the markets sold into, whilst the repairs are done at strategically located, highly sophisticated repair centres in key regions of the world, including Europe. The local depots are essential to service very short replace times, down to 2-48 hours. Customers cannot wait for the exact same part to be repaired but need an immediate replacement, e.g. to minimise any potential network disruption. The part that gets shipped to Europe for repair may therefore not go back to the customer but to a local depot.

Considering the importance of the extensive networks of local depots, to meet the short response times, the exception that it cannot be used when goods are shipped to a customs-free zone / free warehouse is the other main barrier to the use of the EUGEA EU003. This is despite the fact that in this type of closed loop circular economy model, the spare part always remains fully under the control of the exporter and the risk of diversion is consequentially very low. It is not clear why companies implementing a circular economy should not be able to benefit from the general authorisation only as a result of having customers who require advance replacements and repairs. The exception to the EUGEA EU003 should therefore only be applicable when the warehouse is not under the control of the EU exporter (see para 2 point (3) of EUGEA EU003).

4. New Catch-All Controls

DIGITALEUROPE recognizes human rights violations and terrorism, which are global problems that need to be addressed by governments. At the same time, we acknowledge that business must collaborate with governments to resolve these problems. While we support fighting terrorism and violations of human rights, in our view, preventing these undesired activities via very broad catch-all controls will not be effective. Therefore, we recommend an EU-wide list of specific products which are subject to controls adopted at Wassenaar level and an EU-wide list of “sanctioned parties”. We believe that without a list of “sanctioned parties”, exporters will not be able to perform customer screening effectively as it is not possible to match details in the IT system such as name, address of “sanctioned party” or key “red flag” words including “nuclear”, “missile”.

We fully understand the political inconvenience resulting from the publication of a list of potential or real "bad actors" by the EU. Yet, only authorities are empowered and have the adequate means to take such actions. The absence of an EU-wide list of "sanctioned parties" will be inconvenient for exporters having to make such determination based on assumptions instead of factual information stated in regulations. This can negatively impact exporters' relationships with customers and lead effectively to the "privatization of human rights" because business will decide who can and who cannot receive products without specific law listing "sanctioned parties".

Many companies carry out due diligence and have well-established customer policies in place. Despite this, making assumptions about human rights violations or terrorism would be extremely difficult in situations when business does not possess very detailed intelligence about end-users. Making such assumptions, regardless of whether it is a government agency, business, or individual customer, is often simply unrealistic. Existing catch-all provisions are narrower because of the nature of the end-use e.g. they cover military end-use in arms embargo countries and the use of weapons of mass destruction. On the contrary, the new catch-all provisions are very broad, as a wide range of products and technologies can be used in acts of terrorism or violations of human rights. The creativity of "bad actors" does not seem to have limits. Unlike other catch-all provisions, new catch-all controls are more likely to apply to ordinary consumer products and technologies.

In our view, controls should be narrow and realistic. Adding another exception to control products outside of Annex I (see Regulation No 428/2009) raises questions about the effectiveness of the Annex I control list. Export control and trade sanctions compliance checks must be conducted prior to the delivery of an item (hardware, software, technology, service) to avoid an unauthorized, i.e. illegal, delivery. It further is advisable to conduct such checks already in earlier phases of a deal, prior to engaging with a prospect, to avoid that futile efforts are invested into a deal and agreements are signed that cannot be fulfilled.

For ongoing deliveries, e.g. in the Cloud industry, where a certain service is permanently provided, such checks must be conducted on an ongoing basis to ensure that legal changes (e.g. new entries in sanctioned party lists, or new technical controls and/or changes to the product) are conducted as they become effective. Such controls can create very high volumes (e.g. millions of downloads per week, considering all software updates patches). This can only be managed by automation. However, automation requires clear *yes* or *no* decisions. Any ambiguity as proposed in Article 4 (d) ["[…] where there is evidence of the use of this or similar items for directing or implementing such serious violations by the proposed end-user"] requires human assessment and processes and cannot be conducted on a permanent basis. In addition, businesses usually do not have such evidence, unless they are on the ground with the prospective customer. These customer relations usually happen through local sales representatives that may have a culturally different understanding of what is a *serious violation* and that may be biased by sales interests. *Human rights* and *serious violation* are terms subject to interpretation. We believe that such assessments should be in the domain of governments and their services. The latter can issue "lists of concern", which a business can then automatically screen against.

Another question regards the effectiveness of existing catch-all controls and Article 8 of Regulation 428/2009, which allows Member States to deny exports based on national security or human rights concerns depending on how often these mechanisms were used and how effective they were.

Moreover, the interpretation and enforcement of such broad controls can vary across the EU. This means that new catch-all controls can also result in disproportions of export control systems within the EU. We must also stress that, historically, certain law enforcement and other government agencies sometimes misused technology to violate human rights. Without an official list of "sanctioned parties" denials of exports to government customers abroad based merely on assumptions can result in unexpected business consequences. For instance, retaliations may take place and affect trade activities in foreign markets.

Businesses remain fully committed to the protection of human rights and compliance with obligations for export control, often across multiple jurisdictions. However, we are convinced that any extension of controls from a narrow viewpoint will not contribute to international peace and security. To ensure the protection of human rights worldwide, export control of dual-use items should be achieved through consideration of existing mechanisms at the international level e.g. business and human rights Conventions. It may be necessary for the EU to control the export of certain items that may be used to violate human rights. To contribute to international peace and security, such controls should be achieved through existing mechanisms, for instance through the sanctions regimes.

Taking into account all of the above, DIGITALEUROPE recommends the publication of the following:

- An EU-wide list of specific products which are subject to controls (adopted at Wassenaar level)
- An EU-wide list of "bad actors" i.e. "sanctioned parties"

In our view, an EU-wide list of specific controlled items would allow businesses to focus on "high risk" products rather than on a variety of products. However, relevant exceptions should be available e.g. for applications used to protect systems and data. Such a list will be only effective if adopted at Wassenaar level. Otherwise, it will illustrate a diversion from multilateral export control regimes and exports can continue to take place from outside of the EU, which will not resolve the problem in question but rather create competitive disadvantage for EU exporters.

Lastly, we would like to highlight that publishing national lists based on Article 8 of Regulation 428/2009 can lead to further inconsistencies of export control systems across the EU and would result in a diversion from multilateral export control regime. We believe that an EU-wide list of "bad actors" would enable effective customer screening because such a list can be integrated into IT systems at EU level. National lists of "sanctioned parties" can lead to further segmentation of export control systems within the EU.

5. Autonomous List

Annex I.B of the proposed recast includes a new set of products with cyber surveillance technology. These products are set apart from traditional dual-use products that reflect the control lists of other export control regimes of other countries outside of Europe. This proposal for autonomous lists would expand the category of items considered "dual use" in a conceptually troublesome manner. "Dual use" would no longer mean items that actually have civilian and military usage but would now include cyber-security items used for exclusively civilian applications.

The current Regulation, which allows in Article 8 autonomous controls for items with a military application, is consistent with the EU concept of Member State competence in military matters. The new autonomous rule would abandon that historic link and move to a system in which Member States could begin implementing a different law of international trade in civilian goods from that of the EU itself. This invites a proliferation of differing civilian export control lists from one EU Member State to another and moves the Member States in the direction of unilateral national controls outside the Wassenaar regime.

There is, however, a heavy price to pay in terms of clarity and efficacy of export control policy when one ventures down this path. Companies should navigate and determine whether items are sophisticated enough to attract genuine dual-use concerns. Arguably, that is no longer a dual use export control policy, it is a sanctions policy masquerading as though it were a dual use export control policy. Continuing down this path, the effect would be to cast exporters in the role of trying to ascertain whether a common, civilian article they want to sell to a company in a particular country will be used for some type of malicious purpose.

Such a determination is much harder to make than the determination of potential use in making nuclear weapons as contemplated by the dual use definition in Article 2(1) of the current Regulation. The standard that the EU proposal would introduce in the autonomous controls ["can be used for the commission of serious violations of human rights or international humanitarian law"] is much broader and vaguer. A hammer, after all, "can be used" for the commission of serious violations of human rights or international humanitarian law. In other words, the concept of "dual use item" suddenly no longer depends upon the nature or characteristics of the item, but on the subjective intent of the potential recipient of the item. In this respect, this autonomous control provision becomes similar to the catch-all proposal discussed under heading four of this paper.

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's members include in total over 35,000 ICT Companies in Europe represented by 63 Corporate Members and 39 National Trade Associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK