DIGITALEUROPE

European Commission Proposed Recast of the European Export Control Regime

Making the rules fit for the digital world

Brussels, 24 February 2017

INTRODUCTION

On 28 September 2016 the European Commission has adopted a proposal for a Regulation (COM(2016)616) for a modernisation of the EU export controls for dual-use items. This approach includes streamlining the licensing process as well as addressing the latest technological and political challenges facing the European Union.

DIGITALEUROPE and its members are fully committed to the protection of human rights, international peace and security. The ordinary legislative procedure will now see this proposal revised by the European Parliament before agreement and formal adoption together with the Council. Therefore, we recommend that the imminent revision of the proposal must include appropriate changes to satisfactorily resolve these points raised in the paper to avoid unintended consequences.

This paper sets out our suggestions for changes to the proposed Regulation. More details are provided in the annex to this document. These are grouped under three key themes:

1. **Ambiguous definitions and scope**, such as cyber surveillance technologies, licensing criteria, and Intangible Technology Transfers, create legal uncertainty and discourage harmonisation for application of the Regulation across the European Union.

2. **Disproportionate measures**, for example 'Catch-all' controls and technical assistance, create the wrong environment for the operation and growth of digital services and are not fully aligned with the objectives of the Digital Single Market.

3. **Unilateral regimes**, like the proposals for Licence Validity Periods, harm the global competitiveness of European industry and ignore existing international export control regimes with Europe's trading partners without contributing effectively to international peace and security and the protection of human rights.

Throughout the process of public consultation and review of the current Regulation, DIGITALEUROPE has been a trusted partner of the European Commission. We would welcome further opportunities to collaborate with the co-legislators to achieve the best possible controls for the export of dual-use items.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

DIGITALEUROPE Foreword

Designing effective EU Export Controls for Dual-Use Items while maintaining a globally competitive, European industry

The European Union has a well-established industry for dual-use items bringing together thousands of Small and Medium Enterprises (SMEs) and large companies. Dual-use items are often also leading-edge technologies that may be found across a wide range of key sectors of the EU economy. As dual-use items are traded worldwide, the control of dual-use items must be coordinated at a global level to be effective and support the competitiveness of European industry. Therefore, the EU export control regime must continue to be based on the commitments EU Member States have with International Regimes such as the Wassenaar Arrangement; Missile Technology Control Regime; Australia Group and Nuclear Supplier Group.

Unilateral EU action could be detrimental to the global competitiveness of European industry. Without effectively controlling the global availability of dual-use items, the proposed Regulation will not contribute to international peace and security.

The proposed Regulation adopted by the European Commission seeks to create an environment that is balanced, fair, and drives competitive growth within the EU as well as globally. Designing an effective export control regime includes proportionate measures to control the export of items that are extra sensitive. In this respect, DIGITALEUROPE would specifically like to welcome the proposals concerning the adoption of more general export authorisations as this is one of the best ways of creating such an environment.

DIGITALEUROPE Proposals

Precise Definitions and Scope

One of the biggest changes proposed is the extended definition of dual-use items (Article 2) to include cyber surveillance technologies, as well as the inclusion of a new set of products within cyber surveillance technology (Annex 1 B, Category 10).

The new dual-use controls list (Annex 1 B, Category 10) as drafted in the proposal, however, presents an alien element to the existing regime of dual-use controls. Dual-use items are, and should be, identified by their technical characteristics and capabilities and not by their potential misuse. The use of a dual-use item should not trigger the controls but should only be taken into consideration, by the authority, in the decision-making process with consideration for whether an export authorisation may be granted. Whether an application for an authorisation needs to be filed at all, should be based on objective, technical criteria alone. Otherwise the exporter would have the obligation to identify potential end-uses while they do not have the practical or legal means to reliably determine the end-use, especially in the cases of mass market items.

The definition of cyber surveillance technologies is overly broad and ambiguous. This will risk capturing a significant number of essential, legitimate defensive security products and services. Any ambiguity in provisions within the regulation will lead to legal uncertainty for necessary enforcement proceedings, such as administrative or criminal sanctions. The regulation must be readily understandable and provide sufficient legal certainty for it to be effectively enforced in the same way by the judiciary in all Member States.

In addition, the definitions of Intangible Technology Transfers (Article 2(3)b) must be consistent with the revised definition of 'export', the definition of 'exporter' should not include 'making available' data in electronic form, and what constitutes a transmission needs to be clarified. Cloud service providers must be able to distinguish their responsibilities from those of cloud users.

Although we welcome proposals to ensure greater convergence in the application of the regulation across Member States, including alignment on handling licenses and respective processing times (Articles 10 and 14), measures will be required to minimize the scope for different interpretations by Member States of the new licensing criteria in Article 14.

Even though the Commission has stated its commitment to develop guidelines to clarify uncertainties in the Regulation, e.g. on definitions, such guidelines will not provide the legal certainty required. Greater clarity is essential in the Regulation itself. Industry is committed to work constructively with the co-legislators to develop legally clear and technically sound definitions and controls.

Proportionate Measures

Another extensive shift of the proposed Regulation is the changes introduced in the 'catch-all' provision (Article 4). Although DIGITALEUROPE appreciates changes that seek to harmonise the scope and application of the 'catch-all', we believe the proposed changes may have the opposite effect. It is not clear in the proposed regulation when the 'catch-all' provision should be applied and what added value this brings beyond existing controls for the protection of human rights. A 'catch-all' provision for the protection of human rights can only be effective if exporters have clarity over precisely who is targeted. This should be provided by the EU publishing a list of excluded end-users. In the absence of such clarification, exporters will lack the means to distinguish effectively which transactions are subject to control. Other existing instruments such as sanctions will provide more effective means to prevent the export of critical items to high-risk end-users.

The definition of technical assistance (Articles 1.7, 1.9, 5 and 7) risks capturing routine business such as consulting and skills courses. This definition should be narrowly constrained. There should be no extraterritorial controls that would be inconsistent with international law and with the EU's opposition to the exercise of such controls by the US. Likewise, the scope of intra-company transfers as part of EU General Export Authorizations (Annexes) should be expanded.

The proposed regulation expands the List of Controlled items (Annex I, Category 10) to cover products that previously were not controlled as dual-use products and so will now require an export licence prior to export. Consequently, these products are set apart from traditional dual-use products that reflect the control lists of other export control regimes with countries outside Europe (i.e. Wassenaar Arrangement, MTCR, NSG and the Australia Group). This extension of the list would mean that the European Union would unilaterally control products in this technology area as dual-use items.

There is a very real danger that essential, legitimate cyber security technologies or technical assistance services could be included in the scope of export controls or 'catch-all' provisions (Article 4). This would inhibit defensive cyber security measures, increase the likelihood and impact of cyber-attacks, weaken the security of network and information systems, and create a poor environment for digital services in Europe without contributing to international peace and security and the protection of human rights.

Global Viewpoint

DIGITALEUROPE fully understands the concerns related to misuse of digital surveillance and intrusion systems and the need to update export controls in line with technological developments.

Multilateral actions and EU initiatives, such as the different sanctions regimes and the Anti-Torture Regulations, remain the natural policy instruments to deal with these very important issues. Meanwhile, export control regimes should deal with procedures for export of items contributing to proliferation of weapons of mass destruction. Although digital technologies may be used to violate human rights, they also help to protect and empower people to more fully realize their human rights (From exercising their freedom of expression and right to assemble, to economic, social, and cultural rights that improve access to health and education, for example). Digital technologies also enhance democratisation, good governance and rule of law by increasing transparency, imposing international accountability, and fostering cooperation. However, consideration for export controls based on the protection of human rights is provided for in Article 8 of the existing Regulation. Member States may request licences for non-listed items on the grounds of human rights concerns. We believe this legal basis is extensively applied already, and therefore does not require further change.

More specifically as regards the definition of cyber surveillance technologies (Article 2 and Annex 1B), EU export controls should continue to be based closely on the international export control regimes. Adopting unilateral definitions and control categories as proposed will fail to protect human rights and international security since such items will remain freely-available from jurisdictions outside the EU. Such controls will harm the competitiveness of European industry, inhibit the development of defensive cyber security measures, increase the likelihood and impact of cyber-attacks, and create a poor environment for digital services in Europe.

To avoid excessive administrative burdens for License Validity Periods: (Article 10.3), global licenses should be valid for at least 3 years and individual licenses for at least 2 years.

Businesses remain fully committed to the protection of human rights and compliance with obligations for export control, often across multiple jurisdictions. 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, such as the Wassenaar Arrangement. 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.

This is a crucial time for growth of the digital economy in Europe with Industry 4.0, Internet of Things (IOT), and 5G. A unilateral EU list will harm global competitiveness of European industry and restrict international coordination for cyber security measures. The regulation must recognise that cybersecurity is a global issue requiring international cooperation.

Conclusion

The European Commission has clearly identified the Digital Single Market and Digitisation of European Industry among its top priorities to drive growth in the digital economy in Europe. Therefore, we strongly believe that export controls for digital goods and services must precisely focus on proportionate measures considering a global perspective for the most sensitive items.

We believe that any export control currently outside the scope and purpose of the International Regimes to which the European Union is already a Member will have negative consequences for the European digital technology industry. A unilateral viewpoint must be avoided in order to prevent divergence in the global framework for export controls and to stimulate global competitiveness of European industry. Any update of the EU list of dual-use items must conform to commitments that Member States have with export control regimes in countries located outside the EU.

DIGITALEUROPE and its members welcome continued discussion with the European Commission, European Parliament, and Member States. We believe that such an exchange of views, experiences, and expertise between all parties is the best approach to achieve a robust and efficient export control regime in a new digital world.

ANNEX

1. Precise Definitions and Scope

1.1. Export control definition, Cyber surveillance technology and controls

1.1.1. Accounting for new economic realities: The export definition and intangible technology transfers

As export also includes electronic transfers through email attachments, servers up/downloads or even making technology available for an end-user in another country via cloud computing or other internet based sharing platforms, intangible transfer are vital in today's business interaction. These regulations pose challenges not only for licensing but also for enforcement as the traditional control function of physical borders is not applicable here.

The "exporter" definition in Article 2(3)b must be simplified along the lines of the "export" definition in Article 2(2)d by deleting the element of "making available" of software and technology in electronic form. An upload per se (for instance to a cloud server) should no longer qualify as an export and the provision must re-focus on the transmission of such software and technology.

Companies must be able to separate their responsibility from cloud service provision from the accountability of a cloud service user. The user should be responsible for who may download technology and software instead of focusing on the upload or provision of the cloud service. In effect, this would support cloud providers operating multiple cloud services and drive growth in the digital economy in Europe.

1.1.2. Unambiguous and consistent definition

In order to avoid future confusion and uncertainty, the Commission should ensure that the definitions in Article 2 are unambiguous and consistent with one another. For example, the definition of 'Exporter' still contains the wording 'make available', a term that has now been removed from the definition of 'export'. Clearing up this point of confusion will facilitate Industry's ability to comply with the regulation.

1.1.3. Clear-cut definition of cyber surveillance technologies

The Commission's proposal for a definition of cyber surveillance technology in Article 2.21 is very broad, covering any technology which is 'specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system.' Further, it explicitly lists the following items in addition as cyber surveillance technologies.

This includes items related to the following technology and equipment:

(a) mobile telecommunication interception equipment;

(b) intrusion software;

(c) monitoring centres;

(d) lawful interception systems and data retention systems;

(e) digital forensics;

At the outset these products are not necessarily dual-use products, as they have been defined traditionally and in the current Regulation (see Article 2.1).

With the current proposal, a wide array of items could be caught up in the definition, capturing a number of fully legitimate and very needed commercially available cyber security technology products and services. This is firstly because the proposed definition does little to create a distinction between defensive commercially available technologies – critical to the development of Industry 4.0 and Smart Industries - and the offensive technologies that are the primary target of the proposal. This is because the definition does not clarify the meaning of 'specially designed' and 'covert'. Examples of defensive products we believe could be captured include network and endpoint security products that integrate e.g. firewall, VPN, IPS, and other security services into one adaptive, and collaborative defence system. Other examples could be content security tools such as content filtering software, voice security technologies or web and e-mail security technologies. Secondly, 'intrusion software', 'monitoring centres' and 'digital forensics' could also be understood to encompass important cyber security and incident response capabilities such as vulnerability testing tools, sharing of information on unpublished vulnerabilities, and cyber-security monitoring centres. Intrusion software is for example a commonly used vulnerability testing tool to test and understand identified vulnerabilities in legitimate users' IT networks and systems. Likewise samples of malware is routinely used precisely to protect against malware toolkits to e.g. reverse-engineer the malware and thereby develop defences against it. The explicit inclusion of monitoring centres could also have significant repercussions for the ability to continuously monitor and act on cyber security threats as it could be interpreted to include cybersecurity operations centres. It is particularly important to have the ability to monitor, share and react at a global level where the 'follow the sun' model is increasingly standard to provide real time response capabilities. If part of such cyber security services where to be subject to licence regimes this kind of global real time model could be under severe threat.

Blanket licence requirements on any of the above technologies would in short negatively impact legitimate users' ability to defend themselves in an ever-evolving cyber security threat landscape while malicious users are unlikely to be deterred by increased controls nor to experience any decrease in access to any of the technologies. As the threats continuously evolve, the tools to defend against attacks need to evolve with them throughout the lifetime of a product or service. The potential to have to acquire a licence for each further advancement of defence cyber technologies could have detrimental impacts on legitimate users' ability to secure themselves and their IT systems against attacks and exploitations. The broad definition and legal uncertainty does furthermore not only run the risk of increasing controls of legitimate technologies against the political intent, it also makes it difficult for companies to design and implement internal compliance programmes.

1.1.4. New Annex I.B: Aligning the scope on International practices

Our position is that category 10 should not added without being aligned with Wassenaar.

The 'dual-use' scope (Article 2, 1b, 21) has been extended to 'cyber surveillance technology'. Article 2, 1b) states that "cyber-surveillance technology" is relevant for export controls if they "can be used for the commission of serious violations of human rights or international humanitarian law, or can pose a threat to international security or the essential security interests of the Union and its Member States." Initially the European Parliament wanted to prevent certain cases of internal repression in EU third countries. Therefore, the characteristics of the cases should be mentioned in incriminations of the definition: This includes the protection of privacy as well as the protection of freedom of speech/assembly before/during the use of surveillance technology. The scope should also be limited to 'systematic and serious' human rights violations. It is impossible for companies to foresee serious individual cases because everyday goods such as forks or water buckets could be used improperly. It is therefore important to name elements of offence which provide differentiation criteria when an EU third country no longer fulfils its obligation to protect its citizens and rule of law can no longer be guaranteed.

The extension of the 'dual-use' scope is also leading to a new subcategory in Annex I.B listing additional products 'Category 10, "Other Items Of Cyber-Surveillance Technology" for which a licence will be required as per Article 3.

Overview of Specific cyber-surveillance technology controls under Category 10:

Lawful Intercept Monitoring Facilities for LI Systems and specially designed components, and

i) Lawful Intercept retention systems or devices for event data and specially designed components
ii) Software for the use of these items or designed to perform the same function as these items
iii) Technology for these items

The product list contains a very important clarification that 10A001 'does not control systems, or devices that are specially designed for any of the following purposes:

a) billing
b) data collection functions within network elements (e.g., Exchange or HLR)
c) quality of service of the network (Quality of Service - QoS) or
d) User satisfaction (Quality of Experience - QoE)
e) operation at telecommunications companies (service providers)'.

It is essential this list be fully maintained to avoid any inadvertent capture of network equipment and technologies that are capable of networks analysis, diagnostic etc. as these products are an integral and fundamental part of the day to day running of telecom providers' networks.

The most significant and long term impact of the new product list lies however in any further updates to this list. The list can be updated by means of a delegated act, just like Section A of Annex I, in accordance with Article 16. Importantly however, the update of Section B would not be in conformity with relevant international commitments (Wassenaar) but would be amended as necessary out of human rights concerns (Article 16(2)b – in line with the new definition of a dual-use item).

As 'cyber surveillance technologies' are often a usual part of commercial and mass market industrial goods, the non-exhaustive list in Article 2.21 should be aligned on the current discussions at international level (Wassenaar Arrangement), and should not be extended without further discussion and technical consultation with the EU Industry. A unilateral approach executed by the EU Commission may alienate the EU Member States from the Wassenaar Community. IT hardware and software around the world adhere to widely accepted standards. That means that a product or service that is denied an export permit in Europe will most probably be replaced by a competing supplier from a third country. It's essential to have well-balanced and proportionate framework.

Therefore, any unilateral action to amend Annex I or the list of 'other items of cyber surveillance technology' in Annex I.B by the European Commission on its own as introduced in the draft Regulation should be avoided.

1.2. 'Catch-All' Provisions

1.2.1. Ensuring legal certainty for the so-called 'catch-all' clause

As a further way to increase controls on items that can be used for violations of human rights, the Commission is proposing to extend the 'catch-all' clause initially introduced to protect national security:

> *Article 4(1): 'An authorisation shall be required for the export of dual-use items not listed in Annex I if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part:*
>
> *(d) 'for use by persons complicit in or responsible for directing or implementing grave violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination, and where there is evidence of the use of this or similar technology or equipment for directing or implementing such grave violations by the proposed end-user.*
>
> *(e)'for use in connection with acts of terrorism'*

With regard to extending the catch-all clause to serious violations of Human Rights and international humanitarian law, DIGITALEUROPE would like to reiterate its serious doubts that an extension of the catch-all regulation is the most effective instrument to address the underlying issue of preventing the export of critical items to specific, critical countries.

That said, if the dual use regulation is to be extended to more systematically cover issues related to violations of Human Rights, it is essential for industry to know who is targeted and who is not.. In this regard, a truly "targeted" approach is needed by the EU publishing a list of excluded entities or end-users

As it currently stands a licence will be required either if the competent authority has informed the exporter or if the exporter is 'aware' 'under his obligation to exercise due diligence' that the items are or may be intended for HR violations (Article 4(2)). As opposed to the existing provision where controls for non-listed items is based on a minimum of legal certainty, e.g. if the country of destination is subject to an arms embargo, the extension to cover human rights abuse is much more vague and open-ended (e.g. 'serious violations of human rights identified by relevant public international institutions', 'use in connection with acts of terrorism', etc.), leading to legal uncertainty when it comes to application. There may not always be any equivalent objective evidence to 'be aware of', even for companies that do exercise due diligence and invest significant resources, financial

and human, in internal compliance programs. It is therefore not clear what more companies can do or should be expected to do. In this regard, we believe that the term 'aware' should be understood as positive awareness. In the context of the 'catch-all' clause awareness in the sense of specific evidence based on information received directly or indirectly by the exporter that a product will not be used for its usual application but will contribute to the elaboration of weapons of mass destruction or contribute to a military end-use.

The "obligation to exercise due diligence" should be clearly defined to a knowledge criterion such that outside the definition, the exporter has no affirmative duty to inquire, verify or otherwise challenge the intended use of the dual-use item. Further, to avoid potential ambiguity, the 'catch-all' clause should be precisely defined in order to ensure inadvertent controls on commercial technology and software are avoided.

A regulation must be dependable with clear legal rules for it to be effective. Such guaranteed clarity is of paramount importance for the Regulation to be interpreted in the same way by the judiciary in each Member State. Any ambiguity in provisions within the Regulation will lead to legal uncertainty for necessary enforcement proceedings, such as administrative or criminal sanctions. In this regard, we would welcome the introduction of more specific parameters related to the product scope and particularly related to what destinations are considered critical in form of a country list comparable to the US unverified list.

The current Catch-All provisions, Article 4(2), already provide for a country list when, so far military end-uses are concerned, is referring to arms embargo countries.

The above-mentioned terms will need to be specifically defined to ensure inadvertent controls on commercial technology and software are avoided. Rather than shifting the burden to companies, it should be made clear in the Regulation that it is up to the Member States to identify countries of destination where licences for human rights concerns are required. For that purpose, industry should have a common EU list.

Moreover, Article 4, 1e) also extends the 'catch-all' clause to 'acts of terrorism'. Companies would henceforth need to identify use-critical cases where there is a risk that goods will be abused for the purpose of terrorist acts. Hereby companies are expected to perform similar tasks and risk assessments such as intelligence services, state or federal criminal authorities. This will overstrain industry due to the fact of missing evidence and intelligence insights. State bodies should not shift their political responsabilities at the expense of companies. Moreover, there are already existing instruments in the form of the EU anti-terror regulations (sanctioned party lists and sanctions regulations as manifested in Council Regulation (EC) N°881/2002 of 27 May 2002) that specifically address the danger of weapons exports to sanctioned parties or critical countries. In addition, criminal laws of the Member States also prohibit aid to terrorist acts. An unspecific catch-all clause therefore does not offer any added value to the already existing instruments. Moreover, this issue was not addressed in the impact assessment. We therefore stress that the extension in the form of Article 4, 1e) is unnecessary and should be deleted.

1.3. Towards a harmonisation of catch-all licence requirements

Harmonisation is also key. In our experience, Member States have different understanding of what the 'catch-all' is and how it is to be applied. For some Member States, it is seen as a prohibition to export, whilst others regard it as a request for an authorisation to export or the obligation to inform the authorities about the intended export. While today's division of responsibilities between the Commission and Member States should be maintained, a similar approach across the whole Europe is also vital for legal certainty.

The Commission's proposal for a more harmonised approach in the catch-all clause, obliging a Member State that requires a licence for an export to inform the other member states (Article 4(4)). The other member states then have 10 days to raise any objections. Objections from any Member State is to be binding on the issuing member state that shall revoke the licencing requirement, unless doing so would be against its essential security interest. If no objections are received, all Member States shall for the future require licences for all 'essentially similar transactions'.

The Commission correctly identified divergent application of the catch-all clause as problematic for industry as it raises legal uncertainty. However, the current consultation mechanism should be maintained as is but with the addition that authorities that impose a catch-all restriction should duly justify the reasons why towards industry (e.g. in terms of destination, parties of transaction, product's function etc.).

2. Proportionate Measures

2.1. New controls on technical assistance; Extraterritorial application

The regulation also introduces controls on technical assistance to any dual-use item in situations where authorities have determined that supplying technical assistance of the dual-use item may be used in any of the end-use circumstances which trigger one of the catch-all controls (Article 7). Technical assistance is very broadly defined to 'mean any technical support related to repairs, development, manufacture, assembly, testing, maintenance, or any other technical service, and may take forms such as instruction, advice, training, transmission of working knowledge or skills or consulting services, including verbal forms of assistance.'

Due to the broad definitions of technical assistance and of the definition of 'cyber-surveillance technologies', routine business such as consulting, advanced services, TAC support and even industry skills academy courses are at risk of being captured under the proposed technical assistance controls. A narrower definition of cyber surveillance technologies and changes to minimise the scope of the catch-all clause are crucial to avoid the negative impact outlined above. Otherwise companies will be facing significant challenges to identify any potential licensing requirement prior to providing technical assistance, advanced and consulting services as well as engaging in manufacturing and developments partnerships, skills development programs etc.

The EU should also refrain from expanding obligations to those providing brokering services and technical assistance related to dual-use items (Articles 1.7, 1.9, 5 and 7 read in conjunction). In both cases, certain obligations would be imposed on companies that "are owned or controlled" by "any natural or legal person or partnership resident or established in a Member State of the Union". While such obligations would be engaged in relatively limited circumstances, the proposal appears to seek to expand EU jurisdiction, through the Member States, extraterritorially in a manner that is inconsistent with established principles of international law in general and the EU's long-held position. The European Union has repeatedly condemned the United States for seeking to regulate activities by European companies. Going further with these provisions might undermine the EU's ability to maintain a credible opposition to any future attempt by third countries to impose extraterritorial obligations on EU companies.

2.2. Ensuring consistency across Europe and minimising the administrative burden

Consistent licensing practices among EU Member States, including alignment on handling licences (eg Article 10.5), its conditions and respective processing times, would highly boost the competitiveness of businesses in Europe. The long-term ambition should be to convert national general export authorisations to EUGEAs.

It is also difficult to anticipate the effects the new, reviewed, criteria in Article 14 will have. As the criteria set forth in Article 14 are rather vague and could be misinterpreted by the competent authorities in Member States, the level-playing field within Europe might decrease.

We understand that Member States may come to different end results when reviewing an application for a license as they may have different national foreign policies to take into consideration. However, when such a decision is made it should be clear that the decision has been taken due to national foreign policy considerations.

We support the efforts of the European Commission towards more convergence and harmonization of the application of the regulation across Member States.

2.3. General authorisation for encryption and intra-company transfers

The draft regulation introduces a very welcomed 'EU general export authorisations' (EUGEA) for encryption and intra-company transfers.

Encryption is increasingly embedded in every day commercial technologies and helps ensuring secure access to services (e.g. logons, passwords, ATMs, banking online, e-commerce applications), privacy of individuals' and businesses' communications (instant messaging, virtual private networks, webmail) as well as protection of commercial contents (digital rights management for copyrighted material such as DVDs). Tangible privacy and security benefits result from the use of encryption because it mitigates risks related to data confidentiality, integrity and availability.

In order to facilitate secure exports among a parent company and its subsidiaries, DIGITALEUROPE welcomes the Commission's proposal to establish a EUGEA for Intra-Company Technology Transfers (ITT). For internationally active companies, the ability to innovate and offer market-leading solutions and products is closely linked to the free flow of information and technology within companies.

To conduct day-to-day operations, multinational companies export technology, software prototypes, and tools for trade (equipment) to their foreign branches and subsidiaries around the world. To date, these transactions may need multiple export licenses from different export authorities for their own company internal operations, which can negatively impact transactions and hinder fast product development in order to be first to market which is crucial to the competitiveness of European companies.

The current proposal goes in the right direction, but should further be improved by expanding the EUGEA scope to cover collaboration prototypes and tools of trade (equipment) to enable tech companies to ship these items intra company to its subsidiaries. It is important to make sure that intracompany transfers of software and technology are excluded from export controls.

In addition, in order to enable the EUGEA to be used by all subsidiaries of a company across Europe and create a level playing field, the wording of the EUGEA would, however, need to be adapted. As it currently stands, a company will only be able to transfer technology to a non-European subsidiary if the foreign subsidiary is owned or controlled by the exporter. As a consequence, if the foreign subsidiary is owned or controlled by the parent company of the exporting company the EUGEA could not be used.This makes a usage of the EUGEA difficult for companies where the parent company controls or owns (for instance via majority ownership) the different subsidiaries globally.

Effectively this would mean that only the parent company could use the EUGEA whereas its European subsidiaries could not use it, which would contradict the idea of a cross-European use of the EUGEA. Thus, we would suggest to change the wording to the effect that not only the exporters directly owning or controlling the foreign subsidiarity can use the EUGEA, but that the EUGEA can also be used where the parent company of the exporter owns or controls the foreign subsidiarity.

The Commission should also engage Industry in order to determine whether the proposal is sufficiently broad to provide meaningful help with regards to its export needs, including whether the involvement of third party partners would limit the ITT EUGEA's usefulness. Further, the scope of the ITT EUGEA should include movements of third party software or technology stored by customers of cloud service providers.

These additions are an opportunity to harmonise and bring up to date procedures in all Member States that remain inconsistent and unnecessarily bureaucratic. It also bridges the gap with our trading partners who have already a simplified authorisation process.

In any case, it will be important to work with the Industry to help define the technology boundaries between products that are not controlled, those which are controlled via the EUGEA and those specialized products which will require individual export licences.

It should be noted however that as far as cyber security prevention and research is concerned the intra-company transfer exemption will not be sufficient to counter the broad definition of cyber surveillance technology and the potential negative impact on the ability to share crucial information e.g. on unpublished vulnerabilities. As such the general authorisations are welcome and essential but they do not remove the necessity to amend the Commission definition of cyber technology.

3. Global Perspective

3.1. Minimising administrative burdens for Member States and Companies

DIGITALEUROPE welcomes the proposal that the use of global as well as general licenses shall increase. The use of these types of licenses, in general, decreases the administrative burdens on the companies.

However, if the introduction of more of these types of licenses are followed by more reporting requirements the positive effects will decrease as the administrative burdens will only change from before an export has taken place to after. Also, it follows from proposed Article 10.3, that global export authorisations would only be valid for one year. This seems to be an unduly short period, given the time and resources required to renew such licenses in some jurisdictions and the fundamental role that global licenses play in trade management of many large exporters. A duration of 3 years would relieve some of the administrative burdens involved.

Similarly, to avoid excessive burdens for companies, individual export authorisations should be valid for at least 2 years. As the competent authorities in respective Member States may, in accordance with Article 15 (old Article 13) annul, suspend, modify or revoke an export authorization that has been granted, the competent authorities have sufficient tools at their disposal to take appropriate measures against companies that do not fulfil the requirements set forth in a specific license. Consequently, there should be no problem to issue global and individual licenses that are valid for 3 and 2 years, respectively.

3.2. Fostering our cooperation with trading partners

In order to foster an environment that is balanced, fair, and drives competitive growth within the EU as well as globally, the EU Institutions should have regular dialogues and exchange information with third countries, via the Wassenaar discussions but also via bilateral meetings, in order to bring export controls up to the high EU level.

3.3. Privileging appropriate fora for further guidance on respect of Human Rights

Respect of Human Rights and Human Security has always been of utmost importance for DIGITALEUROPE members which have taken actions in many ways – e.g. through the introduction of due diligence programs, reporting in accordance with the UN Guiding Principles on Business and Human Rights and the integration of Human Rights into their corporate culture and ethical guidelines. Multilateral actions and EU initiatives such as the different sanctions regimes and the Anti Torture Regulations remain the natural policy instruments to deal with these very important issues, while Export control regimes should continue to look at establishing good regulatory procedures for export of sensitive goods and services.

3.4. Fixing the Regulation prior to developing guidelines

DIGITALEUROPE cannot stress enough how important it is that the co-legislators introduce amendments in line with the three themes listed above. The European Commission has stated its commitment to develop guidelines to clear up the uncertainties in the Regulation, e.g. around definitions and criteria for use of the catch-all.

This is in industry's view not a desirable solution from a legal perspective. The clarifications should be made in the Regulation itself as guidelines are not legally binding and will not provide the legal certainty required in this very sensitive area. Industry is committed to work constructively with the co-legislators to develop legally clear and technically sound definitions and controls.

--

For more information please contact:
Diane Mievis, Senior Policy Manager for Global Economic Affairs, DIGITALEUROPE
+32 2 609 53 23 or diane.mievis@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's members include 61 corporate members and 37 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

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, 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, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
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