DIGITALEUROPE

Response to EU COMMISSION PUBLIC CONSULTATION GUIDELINES THE EXPORT OF CYBER SURVEILLANCE ITEMS UNDER ARTICLE 5 OF REGULATION (EU) No 2021/821

Introduction

DIGITALEUROPE supports the Commission's work of providing voluntary guidance to exporters to help them understand the human rights implications of exporting items with cyber-surveillance capabilities. However, the Commission should be careful that any guidance it offers does not negatively impact the exporter's ability to make an independent and timely licensing determination. This guidance should rather be operationalised to help EU exporters determine in a standardised manner if a notification to its competent authority is required and what this procedure should entail.

As such, these guidelines should:

- Reinforce the cumulative nature of Article 5 elements.
- Describe when a company should notify its competent authority. We recommend the Commission describes a voluntary process by which a company can determine that a particular export is reasonable, as well as provide a representative list of scenarios, detailing examples of products, end-users, and countries, where the guidance would recommend a company notify or not its competent authority. We recommend this process is accompanied by a decision tree.
- Safeguard predictability, by describing what the notification procedure is. Currently, there is a lack of clarity: what information should be provided, what answer can be given by the competent authority at what time and what is the legal effect of such answers.

More specifically on the due diligence measures, we recommend the Commission updates the guidelines to further clarify:

Item scope and classification

The guidelines currently create additional uncertainty. They should suggest steps that the exporter should take to lift such uncertainty on whether the item is a cyber-surveillance item specified by Article 2 (20) or not such as applying for formal classification with the national competent authority. The guidelines should:

- Align the definition of "specially designed" with current export practices. The new draft guidelines qualify an item as "specially designed" if it is "at least suitable" to enable covert surveillance. This lowers the threshold for items to be considered "specially designed"

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

and diverges from practices that have been established in some Member States since the last recast of the dual-use regulation.[1]

- Potential misuse of the item is also contradictory to the specially designed aspect of the definition of cyber-surveillance items. We suggest references to misuse are removed from the guidelines.
- Explicit that “covert surveillance” is not characterized when data is being transmitted knowingly by the users.
- Make clear that general-purpose computing and networking items such as laptops, servers and their components should not be considered to fall within the scope of unlisted cyber-surveillance items.
- Provide clarity on controls for components by indicating required steps for products that can be used as a component of a larger system.
- In section III.2.1 on facial and emotion recognition, we suggest that the guidelines should explicitly indicate that facial detection is not specified by article 2(20).
- We also recommend deleting the annex on listed items. At best, the annex should reference control text from the Annex I list. These guidelines should be limited to the scope of Article 5 which does not apply to listed items.

On what constitutes awareness/knowledge

- EU Commission should provide examples of documents that can be reviewed and reasonable steps that should be taken to ascertain or lift awareness/knowledge.
- Commission could suggest and include an end-user statement template/language specific to the human rights risk in the annex of the guidelines.
- Multiplication of cross-reference material creates a significant burden the on exporter.
- Guidelines should make it explicit that the exporter’s responsibility is limited to due diligence conducted at the time of export. In the case of components, the exporter would find it extremely difficult and time-consuming to predict and perform due diligence on second-tier and third-tier integration.

On qualification of Internal repression, serious violations of human rights and international humanitarian law

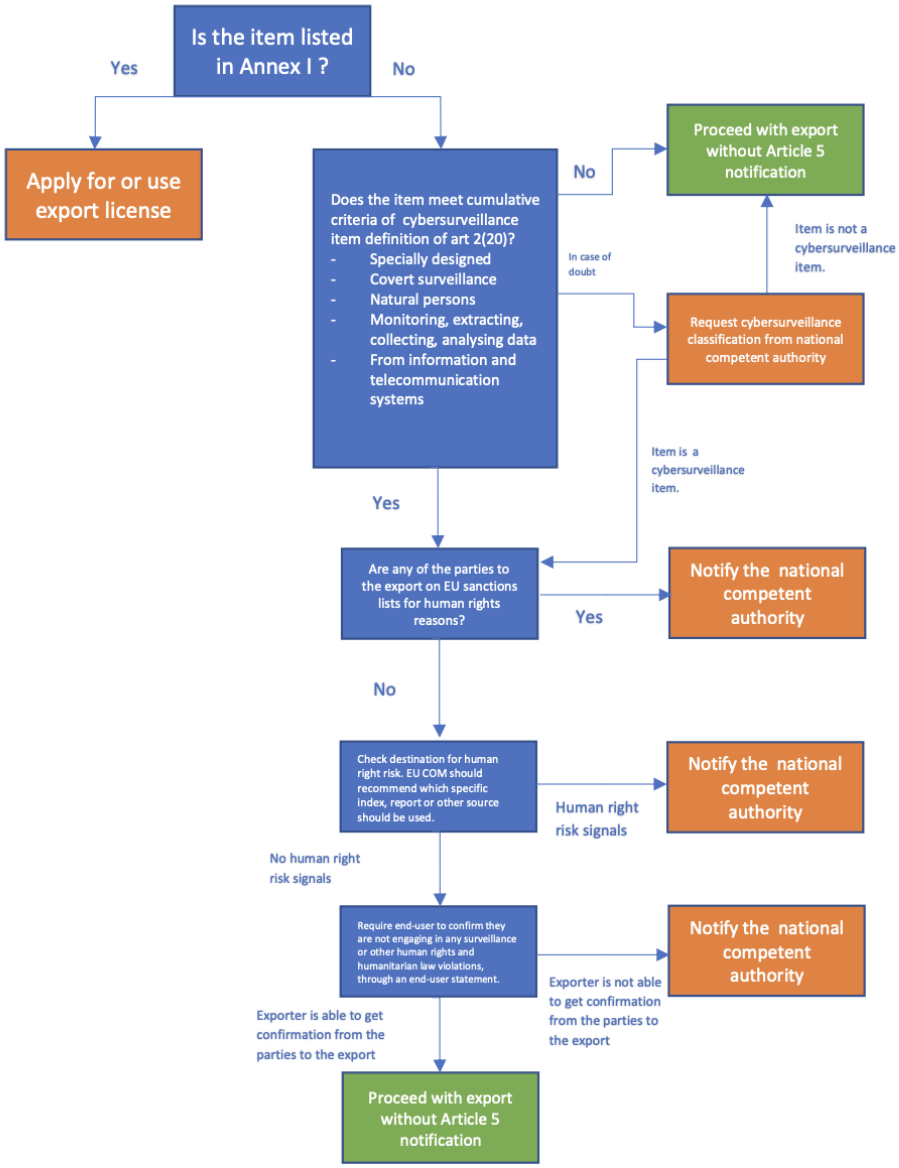
[1] C.f. the Guidelines of the German Export Control Authorities.

- Cross-referenced guidelines such as User's Guide to the Common Position 2008/944/CFSP are directed at Member States and their export licensing officers. Exporters cannot be expected to be able to follow such guidelines. This is a major compliance burden.
- The guidelines must give more specificity on what “an obvious relationship” i.e. Is it ownership? Are state-owned enterprises a good example? Is there a threshold that defines ownership?

On prevention and mitigation of potential future adverse impacts

It is indicated that companies should use due diligence findings to draw up plans to prevent and mitigate potential future adverse impacts. This is an overreach to the usual-use regulation. It conflates with other regulations as well as international human rights norms (e.g., UNGPs). Instead, we recommend the last step of due diligence should be to notify the competent authority. Prevention and mitigation of potential future adverse impacts is the responsibility of the national competent authority in making the notification review as well as an export license decision if applicable.

Accordingly, we would like to recommend the following steps as a basis for a decision tree:



Rather than exporters being responsible for assuming such a heavy compliance burden, we recommend the publication of a harmonised EU-wide list of excluded parties and/or countries of concern, in line with suggestions put forward by various Members States. This would ensure significantly better effectiveness to meet the Commission's goal of preventing exports leading to human rights abuse.

FOR MORE INFORMATION, PLEASE CONTACT:

Cristiana-Amira Cocis

Officer for Digital Trade Policy and International Affairs

cristiana-amira.cocis@digitaleurope

Tsai-wei Chao Muller

Director for Trade Policy & International Affairs

tsai-wei.chao@digitaleurope.org

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 96 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Autodesk, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK