DIGITALEUROPE

15 SEPTEMBER 2022

DIGITALEUROPE Position on Autonomous Controls

Introduction

The current state of play of EU recast Regulation 821/2021 continues to cause concern to the digital technology Industry, in particular with regards to autonomous controls in article 5, 9 and 10. DIGITALEUROPE would like to remind stakeholders that the implementation of the recast regulation should be fit to address the challenges of today without unintentionally undermining European industry's capacity to survive and prosper on the global market.

Recommendations

Expected publication of guidelines on cybersurveillance controls

Delay in publishing guiding principles on cybersurveillance and human rights due diligence sustains the lack of clarity of the new controls and creates a basis for diverse interpretation by EU Member States and exporters risking to unlevel the playing field and in turn make the new controls ineffective.

Call for a harmonised EU-wide list of excluded parties and/or countries of concern

Nevertheless, guidelines cannot replace a clear definition of applicable export licensing criteria. They will not be sufficient to account for automation and enhanced due diligence on the part of the exporters which may be obliged to engage vendors and intelligence service providers to get necessary information. At the very least guidance to exporters should reflect a large span of scenarios addressing different sales channels such as components, indirect and channel distribution models but also more ambiguous customer sectors such as public health, telecommunication service providers etc. They also create a high risk of divergent interpretation by the competent authorities across the EU member

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

states. The European Commission should also strive to be consistent with other regulatory initiatives in this area as to limit the complexity of compliance burden for the industry.

Avoid multiplication of legal instruments

Currently, the EU is addressing these concerns on several fronts. There are proposed or upcoming regulations not only in the area of mandatory supply chain human rights due diligence[1] but also on responsible and ethical AI under the Artificial intelligence Act. We ask that Trade F4 consider these initiatives carefully to avoid overlap, inconsistencies and unnecessary complexity and burden.

Clear alignment with international control regimes on controlled items

We continue to urge stakeholders to work further towards ensuring a level playing field both within Europe and globally, through a clear alignment with the international control regimes such as the Wassenaar Arrangement. The latter have a proven track record of introducing export controls at the global level, including those aimed at addressing human rights concerns. Indeed, a unilateral regime risks harming the global competitiveness of European industry, as well as undermining existing international export control regimes.

EU MS and Commission should work together in Commission Expert Groups (EG) to identify any relevant non listed items and prepare Wassenaar Arrangement proposals to be submitted, advocated for and supported by all MS. On listing additional items with regards to cybersurveillance and Emerging technologies we would like to point out the following:

Item evaluation and selection criteria

To be impactful, goods and technologies to be controlled should be evaluated and selected according to the well-known following criteria:

- the foreign availability of the item outside the EU;
- the ability to make a clear and objective specification of the item;

[1] Corporate due diligence and corporate accountability directive

- the ability to effectively control the export of the goods.

Cybersurveillance items

Any new list controls on cybersurveillance items should be selected and drafted according to above criteria. We would also recommend considering the following elements:

- The positive human rights impacts of the item, including on the rights to privacy and personal security. I.e.: increase online safety and security for users.
- The likelihood of the item to be misused should be taken into consideration in cases where sound product risk analysis shows that although the item or features may present a risk, the likelihood it would actually be used for these reasons is very low as more efficient solutions and options are available to meet the intended effect.

Finally, we would like to elaborate on commercial applications that may be using features that could be regarded as cybersurveillance and how they do not entail a risk of end use in connection with internal repression, nor with the commission of serious violations of human rights and international humanitarian law. Currently the recast regulation identifies the items used for purely commercial applications such as billing, marketing, quality services, user satisfaction or network security. This list of exclusions should be updated following the expansion of commercial implementation.

Emerging technologies

In the same way that recitals on cybersurveillance items acknowledges that commercial items used for purely commercial applications do not present a risk, it should be acknowledged that certain Emerging technologies are not at risk for military-civil fusion. For instance, AI systems with specific transparency obligations should be excluded from any additional controls as they would present a more limited risk to safety or fundamental rights.

Stakeholder consultation periods

Any new controls should be subject to stakeholder consultation with sufficient time provided for analysis and comment to ensure control criteria are understood and implementable by exporters. This consultation could be public or in the context of enhanced engagement in expert groups as described below.

Consistency with other legal instruments

Any additional control should be considered in light of requirements and safeguards from other relevant legal instruments.

General Export authorisations

EU and Member States should consider complementing any new controls with general export authorisations to address export scenarios where the associated risk would remain low.

Avoid over expansion of controls

As export controls compliance frameworks are already complex, EU MS and Commission should also pursue removal of controls where possible. Continuing to control technologies that are now globally available would prevent controls from being effective and listed technologies should be regularly evaluated and removed.

Other multilateral cooperation

Recent cooperation and alignment between the EU and other partners through the EU and US Trade and technology council as well as Coalition response in sanctioning Russia for invading Ukraine have proven to facilitate compliance and have been welcomed by compliance professionals.

Commission should seek to conduct local impact assessment before adopting other countries' unilateral controls. Any new European control should come with comprehensive outreach and capacity building by all participating parties. This would allow to explicit benefits and remaining obligations for European exporters.

This month we set out further recommendations on EU-US TTC opportunities to strengthen cooperation on export controls.

Enhanced cooperation and stakeholder engagement

Enhanced Member State and industry cooperation in STEG/ETEG

It is imperative that the Commission is able to draw on experience and gather input from national competent authorities and industry to paint a complete picture of how controls will work in practice.

We recommend that Member States dedicate relevant resources to participate in these groups. Additionally, industry should be kept abreast of current undertakings and ongoing work. Public sessions could be organised on an ad-hoc basis to keep wider stakeholders informed and allow for public consultation and constructive feedback.

Structured stakeholder engagement and dialogue

We recommend that the Commission EG should be formally composed of representatives from industry and Government representing diverse points of view on the concerns of the exporting community. Such expert groups would be responsible for advising the Commission on the technical parameters for export controls applicable to dual-use commodities and technology and on the administration of those controls on a regular basis. This could be achieved through borrowing from global best-practices such as the United States Bureau of Industry and Security's Technical Advisory Committee, granting a variety of stakeholders the opportunity to apply for a mandate to provide input to ongoing and upcoming initiatives via confidential sessions.

DIGITALEUROPE is ready to continue working constructively with policymakers to make sure Europe can provide a legally sound and operational export control regime for its ICT industry to remain globally competitive whilst still achieving the overall goals of national security and regional stability, protecting citizens from serious violations of human rights, and enabling secure utilization of today's digital tools.

FOR MORE INFORMATION, PLEASE CONTACT:

Luke Makris

Manager for International Outreach Policy

luke.makris@digitaleurope.org / +32493259222

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, Dassault Systèmes, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, 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, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, 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
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: AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK