Federal Office
for Economic Affairs
and Export Control

Leaflet on Art. 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821)

Contents

I. Introduction

Regulation (EU) 2021/821 (“Regulation 2021/821" hereinafter) entered into force on 9 September 2021. It replaces the previous EC Dual-Use Regulation, Regulation (EC) No. 428/2009 (“Regulation 428/2009" hereinafter). With Regulation 2021/821, export control places a greater focus on the protection of human rights.

Already under previous Regulation 428/2009 the competent authorities had to take into account indications as to whether the goods are used for internal repression or other serious violations of human rights (Art. 12 Regulation 428/2009 in conjunction with Criterion Two of the Common Position 2008/944/CFSP[1]), when deciding whether to grant a licence for the export of goods listed in Annex I of the Regulation. This decision criterion continues to apply under the new Regulation (Art. 15 Regulation 2021/821).[2]

In addition, Regulation 2021/821 now includes end use-related controls of non-listed cyber-surveillance items (catch all) that can be used in connection with internal repression, serious violations of human rights or serious violations of international humanitarian law.

The protection of human rights, also through the use of export control, is an important concern of the German Federal Government.

This leaflet is therefore intended to give exporters guidance with the application of Art. 5 Regulation 2021/821. It is a recommendation by the Federal Office of Economics and Export Control (BAFA) that is not legally binding. Investigative authorities and courts may reach a different assessment in individual cases. Moreover, the recommendations of this leaflet have no effect on due diligence based on legislative acts other than Regulation 2021/821 and should not be understood as a limitation of such due diligence. Nor should international guidelines, such as the United Nations Guiding Principles on Business and Human Rights be constrained by this recommendation.

[1] Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment (OJ L 335 of 13.12.2008, p. 99), last modified by Council Decision (CFSP) 2019/1560 of 16 September 2019.

[2] As in the previous Regulation, the Member States also have the option to provide authorisation requirements for human rights considerations beyond those found in the Regulation (Art. 9 (1) Regulation 2021/821). The German Federal Government made use of this option, for example, through the control of data retention systems and equipment (Section 8 (1) no. 2 of the (German) Foreign Trade and Payments Ordinance (AWV) in conjunction with Number 5A902 of Part I Section B of the National Export List).

II. The elements of Art. 5 Regulation 2021/821

Art. 5 (1) and (2) Regulation 2021/821 read as follows:

Paragraph 1

An authorisation shall be required for the export of cyber-surveillance 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, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.

Paragraph 2

Where an exporter is aware, according to its due diligence findings, that cyber-surveillance items which the exporter proposes to export, not listed in Annex I, are intended, in their entirety or in part, for any of the uses referred to in paragraph 1 of this Article, the exporter shall notify the competent authority. That competent authority shall decide whether or not to make the export concerned subject to authorisation. The Commission and the Council shall make available guidelines for exporters, as referred to in Article 26(1).

According to Art. 5 (1) Regulation 2021/821, an authorisation shall be required for the export[3] of cyber-surveillance items not listed in Annex I if the exporter has been informed by BAFA that the items are or may be intended for use in connection with internal repression, the commission of serious violations of human rights and international humanitarian law. Where the exporter is itself aware that cyber-surveillance items not listed in Annex I, which the exporter proposes to export, are intended for any of these sensitive end uses, Art. 5 (2) Regulation 2021/821 obliges the exporter to notify BAFA, which shall then decide whether the export is subject to authorisation.

For exporters, Art.5 (2) Regulation 2021/821 will be most relevant in practice; accordingly, the following remarks on the prerequisites of Art. 5 Regulation 2021/821 also focus on Art. 5 (2) Regulation 2021/821.

Checklist of elements	
Art. 5 (1) Regulation 2021/821	**Art. 5 (2) Regulation 2021/821**
1) Cyber-surveillance items in terms of Art. 2 No. 21 Regulation 2021/821 2) Are **or may be intended** in their entirety or in part for a use in connection with a) internal repression and/or b) serious violations of human rights or c) serious violations of international humanitarian law **3) Notification by the authority** **4) Legal effect:** Authorisation requirement	1) Cyber-surveillance items in terms of Art. 2 No. 21 Regulation 2021/8211 2) Are intended in their entirety or in part for a use in connection with a) internal repression and/or b) serious violations of human rights or c) serious violations of international humanitarian law 3) **Exporter's awareness** based on exporter's due diligence findings 4) **Legal effect:** Exporter has a duty to inform so that BAFA can decide on the authorisation requirement

[3] The word *export* means the shipment or transmission of items to a third country – in other words, to a country outside the customs territory of the European Union (cf. Art. 2 No. 2 Regulation 2021/821). It is to be differentiated from transfer which denotes the shipment and transmission of items within the customs territory of the European Union.

III. Cyber-surveillance items

To meet their due diligence under Art. 5 Regulation 2021/821, exporters must, as a first step, verify whether the items they intend to export are non-listed cyber-surveillance items within the meaning of Art. 5 Regulation 2021/821.[4]

Cyber-surveillance items are defined in Art. 2 No. 20 Regulation 2021/821. Such items are "specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems".

According to Recital No. 8 of Regulation 2021/821, the risk associated with the export of such items relates, in particular, to cases where cyber-surveillance items are specially designed to enable intrusion or deep-packet inspection into information and telecommunications systems in order to conduct covert surveillance of natural persons by monitoring, extracting, collecting or analysing data, including biometrics data, from those systems.

According to Recital No. 8 of Regulation 2021/821, items used for purely commercial applications, such as billing, marketing, quality services, user satisfaction or network security, are generally not subject to control under Art. 5 Regulation 2021/821.

Cyber-surveillance items

1. specially designed to enable the covert surveillance of natural persons
2. by monitoring, extracting, collecting or analysing data
3. from information and telecommunication systems.

At first, the criterion "designed for" means that the item must have already been given a broadened objective during development or design – in other words, it should at least be suitable for and objectively enable the covert surveillance of natural persons. In addition, the emphasis "specially designed" stresses that the covert surveillance of natural persons must have been to the fore during development and design – in other words, the product has been developed mainly for this purpose. The term "specially designed" does not require the item to be usable exclusively for the covert surveillance of natural persons.

Example:

Items for the surveillance of operating status in industry do not constitute cyber-surveillance items in terms of Art. 2 No. 20 because they are not specially designed to enable the surveillance of natural persons.

Items enable covert surveillance of natural persons in particular where, with the help of the items, the surveillance performed is not perceptible to the affected natural person; the affected natural person thus is not accorded the opportunity to orient behaviour to such surveillance. Note that data acquired through open surveillance can nevertheless be covert – that is, diverted, evaluated or processed in another way without the affected natural person having an opportunity to take notice of it. Items enabling such a processing of data from information and telecommunication systems regularly constitute cyber-surveillance items in terms of Art. 2 No. 20 Regulation 2021/821.

Examples:

- Microphones and cameras regularly do not constitute a cyber-surveillance item in terms of Art. 2 No. 20 Regulation 2021/821 even when they can also be used for covert surveillance. The items in question are not items for the surveillance, extraction, collection or analysis of data from information and telecommunication systems.
- Items that can process visual images obtained by cameras from information and telecommunication systems (e.g. evaluation of biometric features) can be items that enable covert cyber-surveillance (e.g. face recognition software).
- Items that enable intrusion into information and telecommunications systems (e.g. intrusion software) or items that enable an analysis of data contained in information and telecommunications systems (e.g. deep-packet inspection) may constitute cyber-surveillance items in terms of Art. 2 No. 20 of Regulation 2021/821.

Note:

Pursuant to Art. 9 (1) Regulation 2021/821 in conjunction with Section 8 Foreign Trade and Payment Ordinance (AWV, hereinafter), an authorisation is also required for the export of items cited in Part I Section B of the National

[4] "Cyber-surveillance items" are not identical with the item list of the US Bureau of Industry and Security (BIS) for "Advanced Surveillance Systems and other items of Human Rights Concerns".

Export List (Annex AL of AWV), irrespective of the proposed end use in the individual case. When an item cited on the National Export List is exported from Germany, the exporter therefore does not have to additionally verify whether the items may be subject to control under Art. 5 Regulation 2021/821.

Only **non-listed** cyber-surveillance items are subject to control under Art. 5 (1) Regulation 2021/821. Art. 3 (1) Regulation 2021/821 already subjects cyber-surveillance items listed in Annex I of Regulation 2021/821 to control regardless of the proposed end use.

On the basis of the structure illustrated in the box below, the following comments are intended to provide exporters with a more detailed illustration which items may be subject to control under Art. 5 Regulation 2021/821.

Cyber-surveillance items that may be subject to control under Art. 5 Regulation 2021/821

1. Items below the control threshold of Annex I
2. Items below the control threshold of Part I Section B of the National Export List
3. Items for surveillance and interception of the Internet and of telephone traffic according to embargo regulations
4. Other items
5. Generally not: Items for purely commercial applications

1. Items below the control threshold of Annex I

When checking whether an item is a cyber-surveillance item in terms of Art. 2 No. 20 Regulation 2021/821, it is advisable to first look at Annex I of Regulation 2021/821. Although, as stated above, cyber-surveillance items that satisfy the criteria of an item listed in Annex I of Regulation 2021/821 are not subject to control under Art. 5 Regulation 2021/821, the item may be controlled under Art. 5 if it comes (just) short of the criteria of a list number.

Cyber-surveillance items in Annex I of Regulation 2021/821

Annex I includes, for example, the following cyber-surveillance items:

1. Systems, equipment and components for the generation, command and control or delivery of intrusion software (Number 4A005);
2. Mobile telecommunications interception and monitoring equipment (5A001f);
3. Internet Protocol (IP) network communications surveillance systems or equipment (Number 5A001j);
4. Software for monitoring or analysis by law enforcement (Number 5D001e);
5. Systems, equipment and components for defeating, weakening or bypassing "information security" to perform "cryptanalytic functions" (Number 5A004a).

Software and technology for the above items are also regularly listed in separate numbers of Annex I.

Items that do not satisfy the criteria required for the above mentioned items listed in Annex I and that may therefore be subject to control under Art. 5 (1) Regulation 2021/821 may be, for example, the following:

- **Intrusion software,** such as malware or Trojans, which conduct covert surveillance of persons through their information systems.
- **Monitoring software** that does not satisfy the cumulative requirements of Number 5D001e – in particular by not offering all functions mentioned in the sub-numbers, such as monitoring software that analyses communication content or metadata, but cannot outline a related network of relationships.
- **Monitoring equipment** that does not satisfy all parameters mentioned in Number 5A001j, such as the delivery of individual operations.
  - ➢ **Note:** In contrast, marketing solutions or network management solutions are regularly not subject to Art. 5 Regulation 2021/821.

Note:

The above list is not exhaustive. Even other cyber-surveillance items that fall short of the criteria set out by Annex I of Regulation 2021/821 may be subject to control under Art. 5 Regulation 2021/821.

2. Items below the control threshold of Part I Section B

Number 5A902 in Part I Section B of the National Export List[5] also contains items that can be classified as cyber-surveillance items. Number 5A902 of Part I Section B of the National Export List cites law enforcement

[5] See attachment

monitoring facilities for lawful interception systems and data retention systems or equipment for event data. Specially designed components for these items are also listed as position 5A902 of Part I Section B of the National Export List.

Items that fall short of the criteria mentioned in the listed position may be subject to control as cyber-surveillance items under Art. 5 Regulation 2021/821. For instance, this may include the following items:

- **Data retention systems** that are used at telecommunications companies and not cited by Number 5A902b.

- **Monitoring facilities** that are neither expressly mentioned in Number 5A902a nor meet comparable standards.

Note:

The above list is not exhaustive. Even other items that fall short of the criteria set out by Part I Section B of the National Export List may be subject to control under Art. 5 Regulation 2021/821.

3. Items for surveillance and interception of the Internet and of telephone traffic according to embargo regulations

Various embargo regulations, such as Regulation (EU) No. 359/2011 (Iran Human Rights Regulation)[6], include restrictions in regard to the export of items for surveillance and interception of the Internet and of telephone traffic. The controlled items are listed in an (identical) item annex to the embargo regulations (see, for instance, Annex IV of the Iran Human Rights Regulation).

In the future it may also be advisable to examine the item annex to embargo regulations when the export is to countries to which the above-mentioned embargo restrictions do not apply. This is because the items mentioned in the item annexes may be viewed as "cyber-surveillance items" in terms of Art. 2 No. 20 Regulation 2021/821 and be controlled under Art. 5 Regulation 2021/821.

For instance, the following items listed in the embargo regulations may be subject to control under Art. 5 Regulation 2021/821:

- **Interception and monitoring equipment for landline, mobile and IP networks**, e.g.:
  - Interception management equipment (IMS),
  - Data retention systems

- **Data analysis equipment for**, e.g.:
  - Deep-packet inspection (DPI)
  - Biometric speaker recognition
  - Pattern recognition and pattern profiling equipment
  - Semantic processing engine equipment

- **Remote forensics equipment**

In individual cases, other items listed in the embargo regulations may also be subject to Art. 5 Regulation 2021/821. This includes, for example, the items mentioned there for jamming communication if they also enable monitoring.

Note:

The embargo provisions that impose end use-independent prohibitions or authorisation requirements for the export of items for surveillance and interception of the Internet and of telephone traffic have priority over Art. 5 Regulation 2021/821.

4. Other items

Items not subject to any of the above case groups may also be cyber-surveillance items within the meaning of Art. 20 No. 20 Regulation 2021/821 and therefore be subject to control under Art. 5 Regulation 2021/821. This also applies to **components, accessories, software and technology** for the aforementioned items – unless they are listed in Annex I of Regulation 2021/821 or Part I Section B of the National Export List and their export is therefore subject to an authorisation requirement under other provisions.

5. Items for purely commercial applications

Note that, although items used for purely commercial applications such as billing, marketing, quality services, user satisfaction or network security, may constitute cyber-surveillance items in terms of Art. 2 No. 20 Regulation 2021/821. Recital No. 8 of Regulation 2021/821 clarifies that such items generally do not entail the risk of end use in connection with internal repression, the commission of serious violations of human rights and international humanitarian law.

[6] As further examples, Annex II of Regulation (EU) 2017/2063 (Venezuela Embargo Regulation) and Annex III of Regulation (EU) 765/2006 (Belarus Embargo Regulation) can be named.

IV. Intended in their entirety or in part for a use in terms of Art. 5 Regulation 2021/821

If the non-listed items to be exported are cyber-surveillance items in terms of Art. 2 No. 20 Regulation 2021/821, the next step is to examine whether the items are intended, in their entirety or in part, for use in connection with internal repression, the commission of serious violations of human rights or international humanitarian law (sensitive end use). The 'connection' depends on the specific objective of the end use of the items in the individual case. The purely abstract risk that the items may be used in a manner that violates human rights is not determinative.

According to Art. 5 (2) Regulation 2021/821, where the exporter is aware that cyber-surveillance items are intended for a sensitive use referred to above, the exporter must notify the competent authority. Unlike Art. 5 (1) Regulation 2021/821 (notification by the competent authority), it is insufficient here that the cyber-surveillance item may be intended for a use referred to above.

Uses in terms of Art. 5 Regulation 2021/821

1. Internal repression,
2. (Other) serious violations of human rights,
3. Serious violation of international humanitarian law.

The sensitive end uses referred to by Art. 5 Regulation 2021/821 are explained in more detail below.

1. Internal repression

The surveillance of natural persons – such as the targeted surveillance of human rights activists or oppositionists – can abet measures for internal repression. According to Common Position 2008/944/CFSP[7], Art. 2 (2) b), internal repression includes, among other things, torture and other cruel, inhuman and degrading treatment or punishment, arbitrary and mass executions, disappearances and arbitrary detentions. Because Art. 5 Regulation 2021/821 requires a connection with internal repression, such cases would be covered by the scope of this provision.

Note:

The use "internal repression" constitutes a subgroup of the use "serious violations of human rights" below.

2. Serious violation of human rights

Cyber-surveillance items can be used not only for purposes of internal repression, but also for other serious violations of human rights. The human rights referred to in Art. 5 (2) Regulation 2021/821 are a part of customary international law and anchored in widely recognised instruments of international law, such as the International Covenant on Civil and Political Rights (ICCPR)[8]. This involves an international covenant, ratified by very many nations worldwide, which enshrines fundamental human rights (and corresponding government obligations). Through publication in the Federal Law Gazette, its content is also accessible to enterprises.[9]

The following, in particular, are among human rights that may be affected by the use of cyber-surveillance items:

- Right to privacy
- Right to freedom of speech, association and assembly
- Right to freedom of thought, conscience and religion
- Right to equal treatment or prohibition of discrimination
- Right to free, equal and secret elections.

Restrictions to the above rights must be in conformity with the international human rights standards. On a regular basis this means that the restrictions must be prescribed by law and serve a legitimate purpose – e.g., be

[7] Council Common Position 2008/944/CFSP
[8] International Covenant on Civil and Political Rights
[9] With the reference to customary international law and the ICCPR it is not implied that enterprises are directly bound to the international human rights guaranteed under international law. Only nations that are contracting parties to the respective international agreements or through customary international law are directly bound to the human rights declared therein and have to live up to their governmental obligation to render protection.

in the interest of a democratic society or national or public security, of the public order, for the protection of public health, public morality or the protection of rights and freedoms of others. In particular, statutes and regulations for the protection of national security may be misused to the detriment of the above rights and, for example, excessively or arbitrarily compromise the right to freedom of expression or privacy.

The violation of human rights must be "serious". Criteria to categorise possible human rights violations as serious can be found, among other places, in the Guide to the Common Position 2008/944/CFSP[10] (Number 2.6). According to this, the nature and consequences of the particular violation are determinative. Systematic and/or widespread human rights violations are regularly viewed as serious. But violations that are not systematic or widespread may be considered "serious" – for example, due to the severity of the intervention. It is not necessary for a public institution, such as bodies of the UN, the EU or the Council of Europe, to have explicitly denoted a human rights violation as "serious".

3. Serious violation of international humanitarian law

International humanitarian law identifies rules, which in times of armed conflicts, serve to protect people who do not or no longer participate in hostilities (e.g. civilians and wounded, sick or captured combatants) (called the Law of Geneva) and impose upon belligerent parties limitations in regard to the means and methods of warfare (called the Law of the Hague). The Law of Geneva is articled in the four Geneva Conventions from 1949 and their Additional Protocols. Also for serious violations of international humanitarian law, the specific objective of the end use of the items in the individual case is determinative.

Example:

Cyber-surveillance items can also be deployed in armed conflict and contribute to serious violations of international humanitarian law, such as in the case of cyber-attacks against the civilian population or through infrastructure that is especially protected by international humanitarian law[11].

[10] User's Guide to Council Common Position 2008/944/CFSP

[11] Thus it may be deduced from Art. 51 (2) Sentence 1 of the Additional Protocol to the Geneva Convention of 12 August 1949 on the Protection of Victims of International Armed Conflicts (Protocol I) and Art. 13 (2) Sentence 1 of the Additional Protocol to the Geneva Convention of 12 August 1949 on the Protection of Victims of Non-international Armed Conflicts (Protocol II) that neither the civilian population as such nor individual civilians may be the target of cyber-attacks.

V. Exporter's awareness and exporter's due diligence

1. Awareness

With the word "aware" a typical regulatory instrument is used to impose end use-related authorisation requirements (catch-all provisions). This is also applicable with Art. 4 Regulation 2021/821. The criterion "aware" is only fulfilled through positive knowledge or awareness which, from a criminal perspective, is to be understood in terms of direct intent. Merely "to deem possible" is not sufficient, so indirect intent or even negligent ignorance do not establish a duty to inform.

However, awareness also exists when the exporter is acquainted with sufficient sources of knowledge from which the exporter can acquire the knowledge in a reasonable way and without special effort. Nor may the exporter deliberately ignore apparent indications; it is improper and may be tantamount to awareness to wilfully look away and intentionally pass up a seemingly obvious opportunity to take not of something which any other in such position would have perceived. The complete failure to perform due diligence is improper ("*passivity does not protect*").

The above-mentioned awareness must be present in the enterprise in the person of the exporter or, in the case of legal entities, the entity's representative. In enterprises it comes down to the awareness of the internal organisation's employees responsible. These can also be from different departments. Because the knowledge of these employees is imputed to the enterprise (Section 166 of the German Civil Code – BGB), it is important that the findings acquired from the transaction-related screening processes are accumulated in one division in the enterprise. Only in this way is it possible to assess whether there is awareness in the enterprise.

Example:

The development department is aware that its product is a cyber-surveillance item and that this is objectively and technically able to be deployed for sensitive end uses in terms of Art. 5 Regulation 2021/821. In the course of a business partner check, the sales department comes across indications that, for the proposed export of this product, the customer (end user) has deployed comparable items in the past for the systematic surveillance of oppositionists.

In this scenario, it is important that this knowledge existing in various areas of the enterprise is accumulated in one division in the enterprise (normally in the export control division) and that BAFA is notified.

2. Due diligence

The due diligence mentioned in Art. 5 (2) Regulation 2021/21 is part of the exporter's Internal Compliance Programme (ICP). It is recommended to undertake measures for assessing the risks connected with the export as part of this due diligence, such as the execution of a three-stage, transaction-related screening process based on item, destination and end-user reference points (on this see (a) below). If the item to be exported or the destination appears on the list published in the Official Journal of the European Union pursuant to Art. 5 (6) Regulation 2021/821, this should certainly induce the exporter to undertake a particularly careful review of the requirements of Art. 5 Regulation 2021/821 (*on this see (b) below*).

(a) Transaction-related screening process[12]

Art. 2 No. 21 and Recital No. 7 of Regulation 2021/821 recommend that the exporters perform a transaction-related screening process as part of its due diligence mentioned in Art. 5 (2) Regulation 2021/21. The transaction-related screening process is a process set up by the exporter whereby the exporter ascertains, assesses and reduces or entirely avoids the risk of serious violations of human rights associated with an export on the basis of information that is already available to the exporter and can be acquired in a reasonable manner and without special effort. Repercussions facilitated directly through the export or to which the export can contribute are to be taken into account.

As the reference to internal repression and the words "in connection with" indicate, not only the direct effects of the use of cyber-surveillance items should enter into the consideration, but also indirect effects of their use or effects to which the items can contribute, such as to torture or against oppositionists.

Note:

Due diligence is a duty to make an effort, not a duty to succeed. This means that enterprises are not obligated to

[12] On the general standards of review, see also COMMISSION RECOMMENDATION (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009.

prevent their items from being used for the violation of human rights or international humanitarian law under all circumstances.

Recital No. 7 of Regulation 2021/821 clarifies that the aforementioned transaction-related screening process is part of the exporter's Internal Compliance Programme (ICP). Regulation 2021/821 describes an ICP as ongoing effective, appropriate and proportionate policies and procedures adopted by exporters to facilitate compliance with the provisions and objectives of this Regulation and with the terms and conditions of the authorisations implemented under this Regulation, including, inter alia, due diligence measures assessing risks related to the export of the items to end users and end uses (Art. 2 No. 21 Regulation 2021/821). Recommendations on implementing an ICP can be found in the BAFA leaflet "Internal Compliance Programmes (ICP) – Company-Internal Export Control Systems"[13] and Commission Recommendation (EU) 2019/1318[14].

Art. 5 Regulation 2021/821 focuses on the end use in the individual case – this means, it is determinative whether, with regard to a specific export, the exporter is aware that the end user being supplied intends the cyber-surveillance items to be exported for a sensitive end use in terms of Art. 5 Regulation 2021/821.

A three-stage screening process, which includes the item to be exported, the destination and the end user, is suitable for determining whether the enterprise has awareness as defined above. The exporter should particularly watch out for red flags in the process. Red flags are unusual circumstances which can give a clue that the items are intended to serve a sensitive end use not intended by the exporter.

When a red flag appears, the exporter is generally not expected to refrain from carrying out the transaction; the exporter should see the red flag as an opportunity to initiate a more in-depth examination and attempt to clarify the circumstances.

Recommendation: Three-stage screening process

1. Item-related
2. Destination-related
3. End user-related

} Screening

(i) Item

Exporters should ensure that they are acquainted with the cyber-surveillance items they export and familiar with their possible uses. If the cyber-surveillance items are objectively and technically able for being deployed in connection with a sensitive end use in terms of Art. 5 Regulation 2021/821, this knowledge (e.g. in the inventory control system) should be documented and made available to the export control division of the enterprise.

Red Flags (by way of example):

- Information (e.g. reports, articles, publications) indicating that a similar item has been deployed in connection with a sensitive end use in terms of Art. 5 Regulation 2021/821.
- The item or a similar item is found on the list published in the Official Journal of the European Union in accordance with Art. 5 (6) Regulation 2021/821 (see Section V, 3).

(ii) Destination

Exporters of cyber-surveillance items should familiarise themselves with the situation in the relevant destination of the items, especially with the general condition of human rights there, as this provides an important indicator of the risk of serious violations of human rights and violations against international humanitarian law connected with an export. If, in the past, in the destined country there were measures of internal repression or other serious violations of human rights – in particular, of the right to privacy, right to freedom of speech, association and assembly and the right to freedom of thought, conscience and religion – or armed conflict prevails in that country, this should prompt the exporter to conduct a careful end-user screening (*see (c) below on this*).

If the exporter has no information on the situation on the country of destination, such as the general human rights conditions there, it is not acceptable for the exporter in the course of its due diligence to ignore information that is obtainable from accessible sources in a reasonable manner and without great effort.

This notably includes the report of the German Federal Government on its human rights policy which outlines human rights conditions in selected countries. Exporters can also use additional publicly accessible sources for country-related screening listed in the Annex of this leaflet.

[13] You can find the leaflet here on the BAFA website.
[14] COMMISSION RECOMMENDATION (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009.

Red Flags (by way of example):

- As can be seen in official reports in particular, persons or groups of persons in the country of destination (e.g. oppositionists, journalists or members of minority groups) are exposed to internal repression measures or other violations of human rights.
- Statutes, regulations or administrative practices in the country of destination unreasonably restrict privacy and/or are directed against persons or members of groups of persons solely for racist reasons or on the basis of ethnic origin, gender, religion or ideology, political opinion or other reasons that are incompatible with human rights.
- In the country of destination, an armed conflict prevails in which cyber-surveillance items were also used in the past.
- The destination is found on the list published in the Official Journal of the European Union in accordance with Art. 5 (6) Regulation 2021/821 (see Section V, (b) below).

(iii) End user

Art. 5 Regulation 2021/821 takes into account the sensitive end use in the individual case. The purpose for which the specific end user intends to deploy the cyber-surveillance items is therefore determinative. The exporter may not deliberately ignore obvious indications in the scope of Art. 5 Regulation 2021/821 which emerge from the person of the end user or from the attendant circumstances of the business relationship with the end user. In particular, exporters should therefore exercise special care when they make deliveries to foreign government end users or to private end users with close ties to government agencies. In such a case – also depending on the general situation in the country of destination (on this, see (ii) above) – it may be advisable to clarify the role assigned to the end user or the government agency to which the end user is closely tied to in the affairs of the state. One question in this context is particularly whether the end user is entrusted with security duties. When there are red flags, information on the intended end use should in any event be obtained from the end user and checked for credibility.

Red Flags (by way of example):

- The governmental end user of the item has security duties or has close ties with (government) agencies which perform security services.
- The governmental end user or closely tied (government) agencies were involved in internal repression measures, other serious violations of human rights or international humanitarian law in the past.
- The governmental end user has – also through cyber-surveillance items – targeted persons or groups of persons solely for racist reasons or on the basis of ethnic origin, gender, religion or ideology, political opinion or other reasons that are incompatible with human rights.
- The end user is part of the armed forces or another group involved in the armed conflict which was involved in internal repression measures, other serious violations of human rights or international humanitarian law in the past.
- Information (e.g. reports, articles, publications), according to which the end user or closely tied (government) agencies have deployed a similar item in the past for uses in terms of Art. 5 Regulation 2021/821.
- The end user has in the past exported cyber-surveillance items to countries where the use of such items has given rise to internal repression measures or other serious violations of human rights or international humanitarian law.

(b) List pursuant to Art. 5 (6) Regulation 2021/821

Under Art. 5 (4) Regulation 2021/821, a Member State that imposes authorisation requirements pursuant to Art. 5 Regulation 2021/821 shall provide the other Member States and the Commission with relevant information on the authorisation requirement in question. The other Member States shall review the submitted information and notify the Commission within 30 days[15] if they would also impose an authorisation requirement for essentially identical transactions. If all 27 Member States give correspondingly positive feedback, the item and, where appropriate, destinations subject to authorisation requirements can be published pursuant to Art. 5 (6) Regulation 2021/821 in a list in the C series of the Official Journal of the European Union. Publication shall occur only if all 27 Member States favourably consent to it. Assumed tacit consent is not sufficient.

If the item to be exported or the destination appears on the list published in the Official Journal of the European Union, this should certainly induce the exporter to undertake a particularly careful review of the requirements of Art. 5 Regulation 2021/821. Inclusion on the list in the Official Journal of the European Union does not automatically result in an authorisation requirement for exporters who wish to transact corresponding exports. An authorisation is required only if the exporter has been

[15] In individual cases the period can be extended for another 30 days (Art. 5 (5) Sentences 3 and 4 of the new EU Dual-Use Regulation).

informed by BAFA in the specific individual case or the exporter is itself aware of a use in terms of Art. 5 (1) Regulation 2021/821. If it cannot be ruled out that the item will be used for serious violations of human rights or for violations of international humanitarian law, BAFA should be involved.

Note:

Where all Member States notify each other and the Commission that an authorisation requirement should be imposed for essentially identical transactions, the Commission shall publish in the C series of the Official Journal of the European Union information regarding the cyber-surveillance items and, where appropriate, destinations.

VI. Legal consequences

1. Exporter's duties to inform

Where in the specific individual case an exporter is aware, according to its due diligence findings, that non-listed cyber-surveillance items which the exporter proposes to export are intended for any of the sensitive end uses in terms of Art. 5 Regulation 2021/821, the exporter is obligated to notify the competent authority pursuant to Art. 5 (2) Regulation 2021/821.

The exporter shall notify BAFA by applying for an export authorisation through the electronic export application system ELAN-K2. The usual application documents are to be included with the application, particularly contract documents, technical documents on the item to be exported, and an End Use Certificate (EUC).

Notification by the exporter enables BAFA to decide on the imposition of an authorisation requirement. If an exporter has notified BAFA pursuant to Art. 5 (2) Regulation 2021/821, it must ensure that the intended export does not occur before a final decision by BAFA.

2. Notification by the authority

Pursuant to Art. 5 (1) Regulation 2021/821, an authorisation shall be required if the exporter has been informed by BAFA that the items in question are or may be intended, in their entirety or in part, for the sensitive end uses described in terms of Art. 5 Regulation 2021/821.

Notification is made by an individual letter to the exporter in which the exporter is referred to the existing authorisation requirement for the specific export in question. The same letter includes the decision of BAFA on the issuance of the export license.

VII. Contact

For questions on the application of Art. 5 Regulation 2021/821, you can contact the BAFA hotline or the dedicated mailbox:

Hotline „Article 5“

Tel.:	+49 (0)6196 908-1444
Availability:	Monday – Friday 09:00 to 15:00 o’clock

Dedicated mailbox:

Email:	Artikel-5@bafa.bund.de

Note:

Comprehensive information on Regulation 2021/821 can be found in the BAFA leaflet on the new EU Dual-Use Regulation “Die neue EU-Dual-Use-Verordnung (Verordnung (EU) 2021/821)” (only available in German).

Attachment

Sources:

- International Covenant on Civil and Political Rights
- Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment
- User's Guide to Council Common Position 2008/944/CFSP
- COMMISSION RECOMMENDATION (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009

Some sources that exporters can use to inform themselves about the situation in the recipient country are mentioned below.

Human Rights:

- Human Rights Report of the German Government (available under www.auswaertiges-amt.de)
- European Council conclusions
- Decisions of the bodies of the Council of Europe regarding human rights violations (e.g. Council of Europe – Human rights)
- Resolutions and reports from the United Nations (www.un.org)

International humanitarian law:

- The Geneva Conventions and their Commentaries
- Rule of Law in Armed Conflicts (RULAC) by The Geneva Academy of International, Humanitarian Law and Human Rights
- Tallinn Manual on the International Law Applicable to Cyber Warfare (print book, subject to costs)
- Guiding Principles on Business and Human Rights

Part I Section B of the National Export List (unofficial translation)

– **2B909** Flow forming machines and machines with combined flow forming and spin-forming functions, other than those controlled by 2B009, 2B109 or 2B209 in the framework of Regulation (EU) 2021/821 as amended, having all of the following characteristics, and specially designed components therefor:
  (a) which, according to the manufacturer's technical specification, can be equipped with numerical control units, computer control or play-back control; and
  (b) a roller force of more than 60 kN, if the purchasing country or country of destination is Syria.

– **2B952** Equipment capable of use in handling biological substances, other than that controlled by 2B352 in the framework of Regulation (EU) 2021/821Regulation (EU) 2021/821 as amended, if the purchasing country or country of destination is Iran, North Korea or Syria:
  (a) fermenters, capable of cultivation of pathogenic 'micro-organisms' or viruses, or capable of toxin production, without the propagation of aerosols and having a total capacity of 10 l or more;
  (b) agitators for fermenters controlled by 2B352a in the framework of Regulation (EU) 2021/821 as amended.
  Technical note:
  Fermenters include bioreactors, chemostats and continuous-flow systems.

– **2B993** Equipment for the deposition of metallic overlays for non-electronic substrates as follows, and specially designed components and accessories therefor, if the purchasing country or country of destination is Iran:
  (a) chemical vapour deposition (CVD) production equipment;
  (b) electron beam physical vapour deposition (EB-PVD) production equipment;
  (c) production equipment for deposition by means of inductive or resistance heating.

– **5A902** Surveillance systems, equipment and components for ICT (Information and Communication Technology) for public networks, not specified by item 5D001e of Annex I of the regulation (EU) 2021/821 as amended, where the destination lies outside the customs territory of the European Union and outside the areas listed in Annex II Section A Part 2 Regulation (EU) 2021/821, as follows:
  (a) Monitoring centres (Law Enforcement Monitoring Facilities) for Lawful Interception Systems (LI, for example according to ETSI ES 201 158, ETSI ES 201 671 or equivalent standards, specifications or standards) and specially designed components therefor,

(b) Retention systems or devices for call data (Intercept Related Information IRI, for example, according to ETSI TS 102 656 or equivalent standards, specifications or standards) and specially designed components therefor.
Technical note:
Call data includes signalling information, origin and destination (e.g. phone numbers, IP or MAC addresses, etc.), date and time and geographical origin of communication.
Note:
5A902 does not control systems, or devices that are specially designed for any 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).

- **5A911** Base stations for digital 'trunked radio' if the purchasing country or country of destination is Sudan or South Sudan.
  Technical note:
  Trunked radio' is a cellular radio communications procedure with mobile subscribers who are assigned frequency trunks for communication. Digital 'trunked radio' (e.g. TETRA, terrestrial trunked radio) uses digital modulation.
- **5D902** 'Software', not specified by item 5D001e of Annex I of the regulation (EU) 2021/821 as amended, where the destination lies outside the customs territory of the European Union and outside the areas listed in Annex II Section A Part 2 Regulation (EU) 2021/821, as follows:
  (a) 'software' specifically designed or modified for the 'development', 'production' or 'use' of installations, functions or performance parameters controlled by entry 5A902;
  (b) 'software' specifically designed or modified for the achievement of characteristics, functions or performance parameters controlled by entry 5A902.
- **5D911** 'Software' specially designed or modified for the 'use' of equipment, which is controlled by item 5A911, if the purchasing country or country of destination is Sudan or South Sudan.
- **5E902** 'Technology' not specified by item 5E001a of Annex I of the regulation (EU) 2021/821 as amended, according to the General Technology Note for the 'development', 'production' and 'use' of installations, functions or performance characteristics controlled by entry 5A902, or 'software' controlled by entry 5D902, where the destination lies outside the customs territory of the European Union and outside the areas listed in Annex II Section A Part 2 Regulation (EU) 2021/821.
- **6A908** Radar-based navigation or surveillance systems for vessel or airborne traffic control, not controlled by items 6A008 or 6A108 in the framework of Regulation (EU) 2021/821 as amended, and specially designed components therefor, if the purchasing country or country of destination is Iran.
- **6D908** 'Software', specially developed or modified for the 'development', 'production' or 'use' of the equipment controlled by 6A908, if the purchasing country or country of destination is Iran.
- **9A904 "**Spacecraft-" and other equipment, as follows:
  (a) Antennas designed for use in connection with "spacecrafts", if the destination is outside the customs territory of the European Union and outside the areas listed in Annex II Section A Part 2 Regulation (EU) 2021/821.
  (b) 'Laser' communication terminals (LCTs, 'laser' data communication stations), other than those specified in 9A004 of Annex I to Regulation (EC) No 428/2009, as amended, for use in connection with "spacecrafts", if the destination is outside the customs territory of the European Union and outside the areas listed in Annex II Section A Part 2 Regulation (EU) 2021/821.
  Technical Note:
  9A904 includes items used in the following contexts with "spacecraft", both on the ground and on "spacecraft":
  1. *Use as a payload for uplink or downlink,*
  2. *Communications between "spacecraft"; or*
  3. *Use in connection with the transmission of telemetry signals.*
- **9A991** Ground vehicles not covered by Part I A of the Export Control List, as follows:
  (a) flatbed trailers and semitrailers with a payload exceeding 25 000 kg and less than 70 000 kg, or having one or more military features and being capable of transporting vehicles controlled by 0006 in Part I A as well as traction vehicles capable of their transportation and having one or more military features if the purchasing country or country of destination is Iran, Libya, Myanmar, North Korea, Pakistan, Somalia or Syria;
  Note:
  Traction vehicles within the meaning of 9A991a comprise all vehicles with primary traction function;

(b) other trucks and off-road vehicles having one or more military features, if the purchasing country or country of destination is Iran, Libya, Myanmar, North Korea, Somalia or Syria.

Note 1: Military features as defined by 9A991 include:

(a) fording capability of 1,2 m or more;
(b) mountings for guns and weapons;
(c) mountings for camouflage netting;
(d) roof lights, round with sliding or swinging cover;
(e) military enamelling;
(f) hook coupling for trailers in conjunction with a so-called NATO-socket.

Note 2: 9A991 does not control ground vehicles when accompanying their users for their own personal use.

- **9A992** Trucks, as follows:
  (a) all-wheel-drive trucks with a payload exceeding 1 000 kg, if the purchasing country or country of destination is North Korea;
  (b) trucks with three or more axles and a maximum permissible gross laden weight of more than 20 000 kg, if the purchasing country or country of destination is Iran or Syria.
- **9A993** Helicopters, helicopter power transfer systems, gas turbine engines and auxiliary power units (APUs) for use in helicopters, and specially designed components therefor, if the purchasing country or country of destination is Cuba, Iran, Libya, Myanmar, North Korea, Somalia or Syria.
- **9A994** Air-cooled power units (aero-engines) with a cubic capacity of 100 cm^3 or more and 600 cm^3 or less, capable of use in unmanned 'air vehicles', and specially designed components therefor, if the purchasing country or country of destination is Iran.
- **9D904** 'Software' specially designed or modified for the 'development', 'production' or 'use' of items specified in 9A904, if the destination is outside the customs territory of the European Union and outside the areas listed in Annex II Section A Part 2 Regulation (EU) 2021/821.
- **9E904** 'Technology' according to the General Technology Note, other than that specified in 5E001b2, 9E001 and 9E002 of Annex I to Regulation (EU) 2021/821 , as amended, for the "development", "production" or "use" of items specified in 9A904 or 'software' specified in 9D904, if the destination is outside the customs territory of the European Union and outside the areas listed in Annex II Section A Part 2 Regulation (EU) 2021/821.
- **9E991** 'Technology' according to the General Technology Note for the 'development' or 'production' of equipment controlled by 9A993, if the purchasing country or country of destination is Cuba, Iran, Libya, Myanmar, North Korea, or Syria.
- **9E992** 'Technology' according to the General Technology Note, other than controlled by 9E101b in the framework of Regulation (EU) 2021/821 as amended, for the 'production' of 'unmanned aerial vehicles' ('UAVs'), if the destination is outside the customs territory of the European Union and outside the areas listed inAnnex II Section A Part 2 Regulation (EU) 2021/821.

Imprint

Publisher
Federal Office for Economic Affairs and Export Control (BAFA)
Division 211 – General Policy and Procedural Issues
Frankfurter Str. 29 - 35
65760 Eschborn
Germany
http://www.bafa.de/

As at
October 2021

Picture Credit
© Maksim Kabakou – stock.adobe.com – Front page

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle ist mit dem audit berufundfamilie für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie GmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.