



Observatoire ARGA

INTERNATIONAL ANALYTICAL REPORT

D-24. Export Controls

Cyber-Surveillance Technology

Regulation (EU) 2021/821 and the ARGA Position

Author:

Sergey Khrabrykh - President of ARGA, PhD

Organization: Observatoire ARGA

Correspondence: 21 rue de l'Aviation, 64600 Anglet, France

Contact: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org

28 September 2026

Contents

Executive summary	3
1. Scope and hierarchy of sources	3
2. Identifying a cyber-surveillance item	4
3. Three distinct thresholds under Article 5	5
4. Human rights and intended end use	6
5. Annex I and technical classification	7
6. Remote access, cloud services and technology transfers	8
7. Transaction participants and jurisdiction	9
8. Establishing the end user	9
9. Risk information and evidential quality	10
10. Engaging the competent authority	11
11. Authorisation and its limits	12
12. Contractual and technical safeguards	13
13. Post-delivery review and change management	14
14. Responding to a report of abuse	15
15. Records and a defensible decision	16
16. Lessons from official measures and case law	17
17. Security research and data protection	18
18. Six practical situations	18
19. The internal programme and accountability	21
20. A decision record for an individual transfer	22
21. Staged delivery and testing safeguards	23
22. ARGA's position and implementation priorities	24
Sources and references	25

Source cut-off: 28 September 2026. Keywords: export controls; cyber-surveillance; Article 5; human rights; end user; due diligence.

Executive summary

Export control of cyber-surveillance technology starts with the capability that a supplier transfers to a particular user. A product name, the purchaser's registration and the existence of a civilian contract do not, on their own, answer that question. A commercial package may combine ordinary network analytics, a controlled module, remote activation of an additional function and integration services. The legal assessment must connect these elements to the technical characteristics, the transfer route and the intended use.

Regulation (EU) 2021/821 establishes two fundamentally different routes to control. For items listed in Annex I, technical classification provides the starting point. For non-listed cyber-surveillance items, Article 5 provides a specific mechanism addressing internal repression and serious violations of human rights and international humanitarian law. Absence from Annex I therefore does not end the assessment. Equally, the theoretical usefulness of almost any software for surveillance does not create a universal licensing requirement. [1-3]

This report develops ARGA's position around three requirements: accurate technical classification, a verifiable assessment of end use and effective action after delivery. The proposed approach does not replace the competent authority's decision with a corporate opinion. It identifies the facts a company should obtain, the way it should resolve inconsistencies and the action it should take while an issue remains unresolved. Commission Recommendation 2024/2659 is used as official but non-binding guidance on Article 5. The report distinguishes its own organisational proposals from the Regulation's legal requirements. [2]

The practical analysis covers the contents of a licensing dossier, intermediary screening, software updates, reports of abuse, six hypothetical transactions and implementation priorities. Particular attention is paid to what the evidence establishes. An administrative listing, a parliamentary recommendation and a judgment have different legal significance. None should be presented as automatically proving a breach of Article 5 in an unrelated transaction.

1. Scope and hierarchy of sources

The report focuses on exports from the European Union of dual-use items capable of enabling covert surveillance of natural persons. It also considers intra-Union transfers, brokering and technical assistance where the relevant operation falls within the Regulation's separate provisions. These regimes cannot be merged simply because they form part of the same commercial project. Each requires its own territorial, substantive and personal basis. [1]

The primary source is Regulation 2021/821 and the applicable amendments to its annexes. Technical classification depends on the control list in force at the time of the operation: an update can change the answer even where the product's commercial name remains the same. Delegated Regulation 2025/2003 updated Annex I; Regulation 2026/1405 corrects certain language versions. The latter should not be described as a separate reform of cyber-surveillance controls. The report uses official materials available as of 28 September 2026. [1, 3, 4]

The next level consists of official recommendations and administrative guidance. Commission documents help explain regulatory expectations, but they do not create a new criminal offence or

displace national rules. French SBDU materials are used to explain the administrative route in France, not as a single procedural code for all EU Member States. US measures are considered comparatively, with attention to their own jurisdictional scope. [2, 5-8]

The method combines interpretation of the legal framework with the design of a decision process that can be independently reviewed. Proposed dossier formats, internal response arrangements and audit criteria are ARGAs recommendations. The six situations in section 18 are hypothetical. They illustrate how different facts change the decision and do not describe actual companies. This permits practical analysis without inventing precedents, refusal statistics or the contents of confidential licensing decisions.

A further distinction concerns the time at which a conclusion is valid. A historical enforcement announcement can establish that an authority took a measure on a particular date. It cannot, without a current check, establish the present restrictions on every named person. Similarly, a classification opinion concerns the described product and legal version. Throughout the report, operational recommendations therefore require current verification at the point of a real transaction.

2. Identifying a cyber-surveillance item

Article 2(20) connects the definition of cyber-surveillance items to dual-use items specially designed to enable covert surveillance of natural persons through monitoring, extracting, collecting or analysing data from information and telecommunication systems. These functions are alternatives: an item need not intercept, retain and analyse data simultaneously. Nevertheless, the ability to process information does not remove the other elements of the definition. [1, 2, section 1.2]

Recommendation 2024/2659 directs attention to objective technical characteristics and the principal purpose of development and design. A product may have several applications while still being specially designed for covert surveillance. Conversely, industrial monitoring or ordinary network protection does not become cyber-surveillance solely because misuse is theoretically possible. The marketing term “security” settles neither question. An engineer must explain the functions included in the version being supplied and the purpose for which those functions were developed. [2]

Covert surveillance is not confined to an invisible installation on a telephone. The Commission's guidance recognises that data acquired in public spaces may subsequently be used in ways that a person cannot objectively anticipate. A visible camera and an undisclosed identification process therefore raise different questions. An ordinary camera should not automatically be classified as a controlled surveillance system. An integrated solution with additional analytics requires assessment of its own characteristics. [2, sections 1.2 and 2.2]

A functional product record is useful in practice. It describes the data processed, the method of identifying a person, access boundaries, modules, remotely activated functions and the operator's actual role. Specifications and a demonstration in a controlled environment support the record. A statement that “no personal data are collected” is insufficient if the system links a persistent device identifier to an individual's movements. Equally, every technical log should not be described as personal identification without examining its contents.

The assessment must address the configuration that will actually be delivered. Where several components are supplied for a known combined use, examining each in isolation can conceal the relevant system capability. Integration does not, however, mean that every general-purpose component automatically acquires the classification of the finished system. The dossier should state the component's role, the known configuration and the legal basis for the conclusion. This supports both positive and negative classification decisions.

A useful boundary test asks what would change the conclusion. If adding an identification module, enabling a hidden function or changing the intended design materially alters the analysis, that event should become a reassessment trigger. The value of a product record lies in these explicit boundaries. A broad assurance covering an entire product family is less reliable than a narrower conclusion that can be matched to a particular release and configuration.

3. Three distinct thresholds under Article 5

The first route is Article 5(1). The competent authority informs the exporter that non-listed cyber-surveillance items are or may be intended, wholly or partly, for the relevant sensitive uses. An authorisation is then required. A company's assessment that the risk is low does not cancel the authority's notification. The exporter must identify the items, user and operation covered by it and ensure that the relevant transfer is not treated as an ordinary commercial release. [1]

The second route is Article 5(2). Where the exporter is aware, according to its due diligence findings, that the items are intended for the specified uses, it must notify the competent authority. The authority decides whether the export should be made subject to authorisation. Notification by an exporter is therefore not the same legal event as an authorisation requirement already triggered by an authority's notification under paragraph 1. Internal procedures should reflect this sequence instead of replacing it with a vague "sanctions risk" label. [1, 2]

The Commission's guidance connects awareness to positive knowledge of intended misuse. A merely theoretical possibility is insufficient. This does not justify passivity: the exporter must take steps to obtain adequate knowledge of the transaction. The practical dossier should distinguish a known fact, a reasoned inference and an unresolved question. An employee's unsupported confidence is not knowledge; deliberately declining to examine available material information is not a sound due diligence process. [2, section 1.2.6]

The third route is Article 5(3). A Member State may adopt or maintain national legislation requiring authorisation where an exporter has grounds for suspecting the specified use. This is an option for national legislation, not an automatically identical EU-wide threshold. The assessment must establish whether the relevant Member State has exercised that option and how. The national suspicion threshold should not be imported into the description of paragraph 2. Nor should the absence of established awareness be treated as permission to ignore an obviously inconsistent transaction. [1]

ARGA recommends an internal hold on the relevant transfer while a material uncertainty is being resolved. Such a precaution may be broader than an express statutory prohibition. The decision should accurately state its basis: an existing licensing requirement, an obligation to notify the authority or a corporate conclusion that the risk is unacceptable. This matters to management and to

the counterparty, which needs to understand what evidence or change could actually alter the outcome.

A hold should also be defined by scope. Restricting the activation of a disputed module need not automatically mean terminating every unrelated service to a customer. Conversely, leaving an equivalent route open can make a nominal hold ineffective. The decision record should identify the capability being withheld, the person authorised to lift the restriction and the facts required for reassessment. These are governance recommendations, rather than additional statutory thresholds.

4. Human rights and intended end use

Article 5 addresses particular sensitive uses, rather than a general moral assessment of a country. Internal repression may involve arbitrary detention, torture and other grave violations of fundamental rights. The analysis should connect the supplied capability, the user's powers and the specific risk. An adverse political context warrants attention but does not, by itself, establish that connection for every transaction. [1, 2, section 1.3]

For example, a system may enable an operator to identify a journalist's contacts with confidential sources. The relevant questions extend beyond technical accuracy. They include the legal basis for selecting the target, the persons entitled to access the results, retention arrangements and independent review. A customer invoking counterterrorism should be asked how its procedure actually limits use of the product and who oversees compliance. General governmental competence is not equivalent to authority for every interference.

International humanitarian law requires separate attention to the context of armed conflict. Not every privacy violation is automatically a violation of that body of law. At the same time, information about civilians' locations can become directly relevant to threats to their lives. The analyst should establish the applicable framework, the user's characteristics and the anticipated use of the data. An emotive description of a technology cannot substitute for that legal and factual work. [2]

Seriousness should be assessed by reference to scale, gravity and the ability to remedy the consequences. A small number of surveillance targets does not make the risk insignificant where torture or exposure of protected sources is at stake. The value of a contract is likewise not a measure of harm. ARGAs proposes recording risk to people separately from risk to the company. Otherwise, a severe human impact may disappear into an average score offset by profitability or market attractiveness.

Human rights due diligence under the UN Guiding Principles has a wider perspective than a single licensing question. It involves identifying impacts, taking action and tracking results. Those principles do not replace the legal conditions in Article 5 and are not a separate export authorisation. Their relevance here is to support attention to consequences beyond the moment of export. [9]

The assessment should examine safeguards in operation, not only their appearance in legislation or a policy manual. Where a user claims that independent approval is mandatory, the company should seek proportionate evidence of how that process applies to the proposed deployment. The objective is not to demand confidential operational files indiscriminately. It is to determine whether the

safeguards relied on in the risk assessment are real, relevant and capable of constraining the supplied capability.

5. Annex I and technical classification

The first substantive check concerns the applicable version of Annex I. The Commission's cyber-surveillance guidance identifies, among other examples, certain telecommunications interception systems, internet surveillance systems, equipment and software associated with intrusion software, and some cryptanalytic and forensic tools. These are signposts, not a substitute control list. The full technical conditions, definitions and notes must be read together. [1-3]

A category cannot be assigned from an industry label. Products described as forensic tools may differ in extraction methods, supported devices and interaction with protective mechanisms. Similarly, the term “intrusion software” operates within particular control entries; it does not mean that all security-testing software is prohibited. A classification opinion should identify the entry, compare the material characteristics and explain any relevant notes. The conclusion needs to be traceable to the actual item.

A classification memorandum benefits from two distinct sign-offs. Engineering is responsible for the accuracy of the technical description; export-control personnel map those facts to the legal text. The product owner confirms what is included in the commercial release. Where a function is inactive but a transferred key can enable it, the record should address that capability separately. A limited demonstration version cannot justify the assessment where the contract actually provides a broader capability.

A change to the control list, product version or material technical parameter should trigger review. For a previously authorised operation, the company checks the authorisation's terms and any applicable transitional provisions. This report does not assume that every update requires a new licence: the answer depends on the transfer and its existing authorisation. Nevertheless, the absence of a physical shipment does not rule out an export of software or technology.

The result must be reproducible. The archive should preserve the list version, configuration, date, responsible specialist and material assumptions. An external opinion is useful where it concerns the actual release and explains its reasoning. “A similar product was previously uncontrolled” does not establish whether the characteristics, transfer route and legal version are the same. The same discipline should apply to a conclusion that no entry is met.

For a product assembled from third-party modules, the supplier's classification is relevant evidence but should not be treated as conclusive for the combined offering. Integration may change what is being transferred, while an inaccurate description of a module can contaminate the entire assessment. The company should obtain enough information to support its own transaction decision and seek authoritative clarification where a material technical question remains unresolved.

6. Remote access, cloud services and technology transfers

The Regulation's definition of export extends beyond physical movement to specified electronic transfers of software or technology outside the Union's customs territory, including making material available in the circumstances covered by the provision. Email, repositories, update servers and remote demonstrations therefore deserve attention alongside equipment shipments. This does not mean that every foreign customer's access to every cloud service automatically constitutes a controlled export. [1, Article 2]

The analysis begins with a transfer map. What does the recipient obtain: an executable module, source code, technical documentation, control of a system or only an output? Where are the relevant object and recipient located? Who decides access? What is the cloud operator's legal and technical role? These questions help distinguish the transfer of a controlled item from a service to which other rules may apply. The server's location alone does not resolve the issue.

For a repository, actual access rights matter. Access may formally be assigned to a European integrator while its team is located in a third country and is authorised to download the material. Conversely, an overseas visitor may receive only a public instruction containing no controlled technology. Both cases require analysis of content and the relevant transfer, rather than a reaction to foreign nationality. EU rules should not be explained by mechanically importing the US concept of a deemed export.

Control should operate before access is granted. ARGA proposes linking the authorised configuration to the account, legal entity, location of use and validity period of the approval. A material change is referred for reassessment. This does not require comprehensive surveillance of employees. Proportionate records of access grants, versions and recipients can establish what capability was actually transferred without collecting unrelated personal information.

Security updates require particularly careful treatment. They may reduce danger to users while also adding controlled functionality. The company should distinguish vulnerability remediation, capability expansion and technical assistance. Where a legal barrier arises, it should discuss lawful remediation with the competent authority. Sending material without assessment in the name of security, or automatically withholding every security fix, is an inadequate substitute for analysing the specific operation.

A remote demonstration should receive the same substantive attention as any other delivery model. The question is whether the recipient obtains a controlled object or capability within the applicable definitions, rather than whether the session is called a demonstration. A narrowly limited presentation and an unrestricted operational trial are different facts. The dossier should preserve the session's boundaries so that the legal conclusion can be matched to what participants were actually allowed to do.

7. Transaction participants and jurisdiction

The exporter is determined by the Regulation's legal criteria, including the power to decide the relevant transfer in the circumstances specified. The entity issuing the invoice does not always answer that question. Within a corporate group, one company may sign the contract, another control the product and a third grant access. The analysis should identify actual authority and actions. An internal agreement can allocate tasks but cannot rewrite mandatory definitions. [1, Article 2]

Intermediary checks should cover commercial function, ownership, actual operators and the capacity to perform the stated project. A reseller without technical staff may have a legitimate business role. However, a demand to conceal the end user, disproportionate remuneration or an unexplained route requires clarification. No single indicator automatically proves circumvention. A combination may nevertheless make the original account of the transaction implausible.

The provisions on brokering, technical assistance and transit have their own conditions. The special Article 5 regime should not simply be applied to every consultation about the same product. Other provisions of the Regulation, national controls or sanctions may still govern the activity. A practical dossier should list separate operations: exporting a module, granting access, training, subsequent support and intra-EU transfer. It should identify the legal basis for checking each. [1, Articles 6-11]

There is no universal freedom to transfer all controlled items within the Union. Annex IV and Article 11 provide particular requirements, while certain circumstances involving subsequent export also matter. Yet the label “cyber-surveillance” does not establish that every intra-Union movement requires authorisation. The conclusion must follow the specific rule. This avoids both unjustified restrictions and the use of an EU intermediary to disregard a known final destination.

A US connection is assessed separately, including the origin of components, whether an item is subject to the EAR, the parties and any other applicable jurisdictional basis. OFAC screening does not replace a BIS analysis, and a European licence does not remove an independent US restriction. Describing these as a single “international ban” obscures the law. Management is better served by several clear applicability conclusions than by one unexplained risk colour.

Where several competent authorities may be relevant, the company should coordinate its submissions consistently. Different descriptions of the same end user or capability can undermine the reliability of the entire process. Consistency does not mean that every authority applies the same rule. It means that the factual record is stable and differences in legal outcome are explained by the applicable regime rather than by selective presentation.

8. Establishing the end user

The most important transaction document is not always the contract with the purchaser. The end user may be a public authority or operator that the contract does not expressly identify. ARGA proposes distinguishing four roles: the payer, the recipient, the system operator and the person or body deciding whom to place under surveillance. Where these roles are separate, the explanation should be supported by evidence and match the deployment architecture.

An end-use statement should describe the function, operating location, operators and limits on onward transfer. A generic statement that the item is for “national security” is too broad to test

meaningfully. A more useful document identifies the unit's mandate, permitted tasks, process for approving access and restrictions on transfer to other operators. The statement remains evidence of the customer's representation, rather than independent proof that the representation is accurate.

Consistency across sources matters. If a telecommunications company procures the system but a different government unit requests training, that unit's role needs to be established. If the number of licences greatly exceeds the stated unit's needs, the project architecture requires explanation. There may be an innocent technical reason, but it must be specific. An intermediary's assertion that a practice is customary in the local market does not identify the actual operator.

Ownership and control checks are especially important for sanctions, but a beneficial-ownership chart is not a substitute for investigating use. A fully transparent company may serve a problematic end user, while a complex group may have a legitimate structure. Corporate form should not create a presumption of wrongdoing. The conclusion should rest on the facts as a whole. A refusal to provide material information is relevant because it may prevent a sufficiently supported positive decision.

A government customer may invoke secrecy. The supplier need not demand the identities of operational targets, but secrecy cannot simply remove the end-use assessment. Possible approaches include confirmation of powers through a competent authority, restricted access for an independent reviewer and a description of oversight that does not disclose operations. If even minimum information about the user and purpose cannot be obtained, the company should recognise that limitation and consult the regulator or decline the transaction.

The process should also distinguish a customer's legal authority from its technical access. A unit may have a statutory mandate but allow contractors or other agencies to operate its system. Conversely, a technical administrator may maintain infrastructure without deciding surveillance targets. Both arrangements are possible, but each requires a clear account of responsibilities. Identifying the purchasing body alone leaves these operational questions unresolved.

9. Risk information and evidential quality

A dossier should not become a collection of adverse media articles. For each material report, the company should record its author, date, primary source, period covered and connection to the specific entity. Several publications repeating one investigation are not several independent confirmations. A denial should also be assessed for substance: supporting documents carry more weight than a general rejection that does not answer the identified facts.

A technical investigation may reliably identify traces of a particular tool without establishing the customer, operator or lawfulness of a specific deployment. The report should distinguish attribution to a product, infrastructure and responsible person. A mistake can harm both the surveillance target and an incorrectly accused company. For an export decision, serious unresolved uncertainty may justify a precautionary hold even where the evidence is not sufficient for a public allegation.

ARGA proposes an unresolved-issues register. Each entry records the fact, its potential significance, the source, the clarification needed and the person responsible. A deployment-address mismatch should not simply be labelled "high risk". The record should explain why it might indicate a

different operator, what confirmation has been requested and what transfer is temporarily restricted. This permits review of decision quality rather than the number of pages collected.

Risk should not always be averaged. Established intent to use a capability to persecute a particular group is not neutralised by the buyer's sound financial statements. Conversely, a weak unsubstantiated signal should not permanently exclude a lawful customer. Each conclusion should have reassessment conditions: independent confirmation of the end user, a changed configuration, a competent authority's decision or correction of a false screening match.

Evidence gathering must protect sources. The supplier should not forward a complainant's identity or details identifying a victim to a potential surveillance operator merely to obtain comment. Questions to the counterparty should test the material issue with minimum disclosure. Where a safe check cannot be undertaken, that limitation belongs in the decision. It cannot be compensated for by creating a new risk to the person who reported the concern.

A useful final review asks whether the conclusion is stronger than the evidence. "The product was probably involved", "the customer operated it" and "the customer used it unlawfully" are progressively different propositions. The decision-maker should know which is supported and which remains an inference. Internal precautionary action can be justified without presenting an uncertain proposition as a proven fact, provided the action's basis is accurately recorded.

10. Engaging the competent authority

In France, SBDU acts as the competent authority for classification and export licensing of dual-use items. Its official materials identify technical descriptions, contractual records and information about final use among the documents relevant to the applicable procedure. A promotional brochure alone is unlikely to explain a complex operation. The authority needs to understand the actual transaction, not just the applicant's business sector. [5-7]

The ARGA dossier begins with a short statement of the decision sought. The company specifies whether it is requesting classification, notifying under Article 5(2), applying for a licence or reporting a change to an authorised transaction. The supporting record then provides the functional product description, participant map, transfer route, end-use assessment and material inconsistencies. Legal arguments should be accompanied by the evidence needed to test their factual premises.

Adverse information must be presented fairly. If an internal conclusion depended on a disputed fact, that fact should not disappear from the submission merely because it complicates approval. The company should identify the source, its reliability assessment and the customer's response. Unknown matters should remain labelled as unknown. The authority may possess additional information; concealing a material question defeats the preventive purpose of the process.

Dossier component	What it establishes	Operational value
Product and release	Functions, modules and technical parameters	Reproducible classification
Parties and route	Recipient, operator, intermediaries and access	Applicable control regimes
Intended end use	Task, legal basis and limitations	Assessment of potential misuse
Due diligence findings	Sources, responses and unresolved issues	An informed authority decision
Delivery conditions	Stages, updates and transfer controls	Ability to comply with authorisation

Correspondence with the authority should be preserved with the relevant dossier version. Where a response is based on a particular configuration, a different user or functionality requires checking whether that response still applies. Preliminary guidance should not be represented as an unconditional licence. Nor should the company invent a deadline after which silence becomes approval unless the applicable law expressly gives silence that effect.

The submission should make technical complexity understandable without concealing it. A concise description can explain what a module enables, who will operate it and which safeguards limit its use; detailed specifications can support that account. Replacing technical facts with reassuring language makes the application harder to assess. Conversely, supplying a large unstructured document dump can obscure the very issue on which the authority is asked to decide.

11. Authorisation and its limits

Article 15 requires relevant considerations to be taken into account, including international obligations, sanctions, foreign and security policy considerations, intended end use and diversion risk. A licence is therefore not merely a certificate of technical conformity. Its type and terms determine the operations, recipients, quantities and period covered. Eligibility to use a general authorisation likewise depends on that authorisation's conditions and exclusions. [1]

A licence record should be available to the people executing the transaction. It should identify the permitted release, user, country, validity period, support restrictions and reporting steps where applicable. An accountant seeing a licence number is not enough: an engineer must know which functions may be activated. If the conditions are unintelligible to the delivery team, the risk of non-compliance remains even where the legal archive is carefully maintained.

A dual-use authorisation does not establish compliance with data-protection rules, the lawfulness of surveillance in the destination state or the absence of a sanctions prohibition. In France, cryptography regulation and ANSSI's responsibilities also require a separate assessment under the relevant rules. An SBDU export licence should not be presented as universal permission for every aspect of the product. [8] Separate analyses clarify exactly which question remains unresolved.

Material changes after approval cannot be ignored. New information about the user, a different route or additional functionality may require consultation with the authority, reconsideration of the company's decision or other action under the authorisation's terms. A licence should not be assumed to legitimise every future supply to the same customer. Each operation must remain within its factual and legal boundaries.

An internal refusal may remain possible in the absence of an express legal prohibition. A company may adopt a stricter policy while respecting its applicable contractual and other obligations. Accurate wording is especially important: the refusal should be attributed to the corporate standard or unresolved risk, rather than a fictional governmental requirement. This improves communication with the counterparty and preserves the distinction between law and organisational policy.

Where a licence contains a reporting or end-use condition, compliance needs an operational owner. The task should not disappear between legal, logistics and engineering teams. The record should show when the condition is checked and what evidence demonstrates completion. A condition that exists only as text in an archived licence is vulnerable to failure during subsequent updates, staff changes or integration by a third party.

12. Contractual and technical safeguards

A contract should preserve the assessed model of use. It should define the agreed user, configuration, operating territory and procedure for changing these parameters. A prohibition on unlawful surveillance is useful but too general if nobody is responsible for demonstrating compliance and the supplier has no means of checking it. The practical objective is a clear obligation paired with an enforceable verification mechanism.

ARGA recommends restrictions on unauthorised onward transfer, notice of operator changes and a right to suspend relevant deliveries where a material inconsistency arises. The supplier's powers should not be unlimited. Document-request procedures, response periods, protection of confidential information and independent review can make the arrangement workable. A unilateral right to demand any information at any time often proves less useful in practice than a precise, proportionate clause.

Technical measures should be judged against the identified risk. Separation of operator permissions, limits on activated modules, configuration-change records and separate approval for expanded access may be more effective than a general promise of ethical use. A geographical restriction does not guarantee that information will not be used against someone elsewhere. The assessment should explain which risk the measure reduces and which remains.

Remote disabling is not a universal answer. It may introduce a vulnerability, conflict with contractual rights or harm legitimate users. If provided, it requires defined triggers, authority, a safe execution process and an assessment of consequences. Control should not depend on a hidden capability unknown to the responsible parties. Technical ability to stop a system is also distinct from the legal authority to exercise it.

A contract cannot erase knowledge of intended misuse. Where material facts indicate a sensitive purpose, a signed standard declaration does not automatically return the transaction to a low-risk category. A genuinely changed configuration may, however, affect the conclusion. Removing a

disputed module and independently verifying its removal has a different evidential value from a promise not to activate it. The modified transaction should be reassessed and documented.

Contractual remedies should account for the supplier's actual leverage. If the product is permanently installed and operates independently, a promise of future cooperation may be difficult to enforce. That limitation should influence the initial risk assessment and the decision to supply, rather than being discovered only after an incident. No contractual language can manufacture technical control or legal access that the supplier does not possess.

13. Post-delivery review and change management

Risk evolves with the product and the customer. A system acquired for one purpose may receive additional modules, pass to another operator or be used in a changed political environment. A first-sale-only review is therefore an inadequate organisational model. Article 5 should not, however, be described as an unconditional requirement to monitor every customer action continuously. Specific legal duties follow from the legislation, licence and applicable national rules.

ARGA's proposed model is event-based. Reassessment is triggered by a different end user, a material expansion of functionality, a new access route, a credible report of abuse or a change in the applicable restrictive regime. The commercial team reports events but does not decide alone whether to continue. Routine renewal of an unchanged service may justify a lighter review than a new deployment where the continuing accuracy of the information supports that approach.

Support engineers often see inconsistencies first. Requests to alter logging, expand the number of operators or move activation to another country may be material. An engineer should not be turned into an investigator. The task is to record the actual change and refer it to the responsible specialist. A clear reporting form and a review process protected from inappropriate sales pressure make this feasible in daily work.

Where an item operates autonomously and the supplier no longer has access, comprehensive end-use control should not be promised. The dossier should state those limits. Possible measures include periodic user confirmations, independent audits and conditions on future capability upgrades. Their selection depends on risk and practical enforceability. The absence of perfect monitoring does not justify false claims that it exists.

Support restrictions must consider the harm they may cause. Declining new capabilities and declining a vulnerability fix have different consequences. The decision should specify the activities suspended, the steps needed to maintain safety and whether consultation with the authority is required. Precision helps avoid an attempt to prevent misuse causing a data breach or destruction of relevant evidence.

Event-based review also needs a route back to ordinary operation. Once a concern has been resolved, the responsible person should record the evidence, reassess any remaining conditions and communicate the outcome to delivery teams. Otherwise, obsolete restrictions can remain in place indefinitely or be lifted informally without a decision. Both outcomes weaken the credibility of the control system.

14. Responding to a report of abuse

The first step is safe receipt of information. A reporting channel should allow material facts to be submitted without forcing the person's identity into public view or disclosing it to a potentially implicated customer. The organisation should explain confidentiality limits and avoid promising absolute protection that it cannot provide. Access to the material should be restricted to those who need it for assessment and decision-making.

The company then records when the report arrived, its contents and the technical material available. Originals should be preserved separately from working copies, with transformations and access documented. The reviewer determines whether the report concerns the company's product, which version and what period. A complainant should not be required to prove the entire chain of responsibility before an initial assessment begins. Technical plausibility and potential danger to a person may justify immediate internal escalation.

One early task is to check forthcoming transfers. If expanded access for the potentially relevant operator is scheduled for the next day, the decision cannot necessarily wait for a months-long investigation. A temporary hold on that expansion may be a reasonable corporate precaution. The legal team should concurrently assess duties to competent authorities, licence conditions and applicable data rules. This report does not invent a universal notification deadline for every possible incident.

Contact with the counterparty should follow an assessment of the risk to the complainant and the evidence. Questions should address a specific inconsistency instead of forwarding the entire report. An unsupported response remains an unresolved issue. A response that genuinely disproves the initial concern may justify reconsidering a restriction. The process must allow either result: its purpose is a reliable decision, not mandatory confirmation of the first suspicion.

Closure should include corrective measures and consideration of appropriate assistance to affected people. Depending on the facts, that may involve preserving evidence, cooperating with a lawful investigation, changing the product or supporting safe remediation. Not every company can determine compensation or disclose classified material. The UN Guiding Principles inform responsible conduct; applicable law determines specific legal duties and remedies. [9]

A useful closure record distinguishes facts established, facts unresolved, action taken and the basis for future review. It should avoid declaring a complaint unfounded merely because operator attribution was impossible. Equally, an unresolved allegation should not be repeated as a proven finding. The company can acknowledge evidential limits while still explaining how it has addressed the risks within its control.

15. Records and a defensible decision

Article 27 requires detailed registers or records of export operations and the relevant supporting documents. For the records identified there concerning exports, brokering services and technical assistance, retention is at least five years from the end of the calendar year in which the operation took place. Intra-Union transfers have their own requirements. A single retention formula should not be applied to the entire archive without checking the relevant provision. National and other applicable duties may require further retention. [1, Article 27]

A useful legal record shows the basis of the decision at the time it was made, not only its outcome. It contains the product version, classification, user documents, material sources, answers to questions, authorisation conditions and actual transfers. Information discovered later should be added with its date, rather than substituted into the original record. Otherwise, a reasonable decision based on limited information cannot be distinguished from a retrospective justification.

The archive should be proportionate to its purpose. Export control does not by default require the supplier to retain the contents of all communications of people observed by its customer. Such accumulation creates its own risk. Where the GDPR applies, the company must establish a lawful basis, minimise the data, restrict access and use justified retention periods. The possibility of litigation does not permit indefinite storage of unrelated information without a connection to a specific need. [15]

Digital evidence matters at the level of actions: who approved access, when a version was activated and which recipient received documentation. Hashes and logs can help establish integrity, but they do not prove the truth of an original statement or the lawfulness of obtaining it. Technical integrity, factual reliability and legal admissibility are different questions. An internal review should address each where it matters to the operation.

Preservation during an incident should be targeted. The responsible person identifies relevant documents, prevents routine deletion and controls access. Complying with a lawful governmental request and voluntarily sending material to a foreign counterparty have different legal bases. Protection for legal advice also depends on the applicable regime. Labelling an email “privileged” does not, by itself, create privilege.

The decision record should remain understandable to someone who did not participate in the transaction. A sequence of approvals without the underlying reasons is weak evidence of a real assessment. Conversely, a concise explanation supported by preserved source material can demonstrate both the scope of the review and its limitations. The aim is not maximal documentation, but a reliable account of the facts, law and judgement that produced the outcome.

16. Lessons from official measures and case law

In November 2021, BIS announced the addition of NSO Group and Candiru to the Entity List, referring to evidence concerning spyware supplied to foreign governments and used against journalists, activists and others. The measure addressed transactions involving items subject to the EAR under the specified licensing conditions. It was a US administrative export-control action, not a judgment establishing a breach of European Article 5. A transaction assessment must separately check the current entry and jurisdictional connection. [10]

On 5 March 2024, OFAC announced sanctions against two individuals and five entities associated with the Intellexa Consortium. The US Treasury explained the action by reference to commercial spyware risks and deployment, including threats to US persons. This historical action illustrates the independence of financial restrictions: the product's export classification and a participant's sanctions status answer different questions. It does not establish identical restrictions on every industry participant. Current status must be checked when a transaction is assessed. [11]

The European Parliament's recommendations following the PEGA inquiry in June 2023 addressed independent investigations, safeguards, remedies and enforcement of export rules. The document matters as an institutional assessment and a statement of policy priorities. It does not replace an individual licensing decision or establish the criminal guilt of every person mentioned in the inquiry. Its use requires a clear explanation of its legal nature. [12]

In *Big Brother Watch and Others v. the United Kingdom*, the Grand Chamber of the European Court of Human Rights examined interception safeguards and related issues under Articles 8 and 10 of the Convention on 25 May 2021. It identified deficiencies including independent authorisation, the treatment of selectors linked to individuals and protection of journalistic material. The judgment is not an export-licensing case. Its relevance here lies in assessing safeguards throughout the handling of information. [13]

ARGA draws an organisational lesson from these materials: examine constraints on actual deployment as well as the stated purchasing purpose. This is the report's analytical conclusion, not a quotation from a single international rule. An administrative measure can create binding restrictions within its jurisdiction; a judgment explains the legal standard in the context decided; a parliamentary recommendation identifies a systemic concern. Conflating those functions produces a less reliable legal analysis.

These examples also caution against using enforcement history as a substitute for transaction analysis. The relevant question is not whether a business belongs to a controversial sector, but what legal measures and substantiated facts apply to the actual parties and capability. Historical information can be highly material while still requiring current verification. A sound dossier preserves both its significance and its limits.

17. Security research and data protection

Controls should preserve the distinction between abusive capabilities and legitimate security research. Annex I contains definitions and specific notes relevant to vulnerability disclosure and cyber incident response. Their application depends on the particular control entry and material transferred. An exclusion for a specified technology or activity should not become a blanket exemption for every product marketed as cybersecurity. [1]

Commission Recommendation 2021/1700 concerns internal compliance programmes for research involving dual-use items. Universities and laboratories can benefit from early project classification, allocated responsibility and assessment of international exchanges. Academic affiliation does not automatically establish that every transfer is basic scientific research or information in the public domain. The content and applicable definitions remain decisive. [14]

A research procedure should be sufficiently responsive to support responsible remediation. ARGA proposes an identified contact, a minimum description of the proposed transfer and a route for urgent legal assessment. The researcher explains the purpose and nature of the material without disclosing dangerous detail to an unnecessarily broad group. The decision should identify the actual basis for permissibility, rather than relying on general trust in the sender's profession.

Data protection remains a separate workstream. A product transfer and a personal-data transfer may occur together, but one authorisation does not replace the other. Where the GDPR applies, the legal basis, purpose, minimisation, security and conditions for international transfers require assessment. Regulation 2021/821 should not be understood as independently authorising a supplier to collect data about surveillance targets for a corporate audit. [15]

Compliance checks should not increase the harm they seek to prevent. Instead of taking a complete surveillance dataset, the reviewer may be able to use limited administrative logs, independent sample-based confirmation or genuinely anonymised measures. The method must answer the relevant question. If supposed anonymisation permits a person to be reidentified, it is not an adequate answer simply because the dataset has been labelled anonymous.

A practical boundary is necessary between describing a vulnerability for remediation and transferring a broader operational package. The first activity may fall within a relevant definition or note, while the second may raise additional classification questions. Treating the whole package identically because it originated in one research project can either overrestrict legitimate exchange or overlook controlled material. A component-by-component analysis, followed by an assessment of the combined transfer, is more reliable.

18. Six practical situations

Situation 1. Ordinary network diagnostics

An EU supplier sells a telecommunications operator a load-measurement system without functions designed for covert surveillance of people. Engineering confirms the configuration, and there is no information indicating a different purpose. Annex I is checked because a network product may meet a separate entry through its technical characteristics. If no relevant ground is found, the word “monitoring” does not, by itself, turn the system into a cyber-surveillance item under Article 2(20).

The decision records its limits: the recipient obtains the diagnostic module, and additional functions are not activated. A later request for individual profiling receives a separate assessment. The practical lesson is that a negative conclusion must be technically supported and confined to the reviewed configuration. It is not an indefinite certificate for the entire product family.

The evidence that would change the decision should be explicit. A new module, different functional specification or credible indication that the supplied configuration was inaccurately described would require review. A general adverse view of the destination, without more, should not be retroactively substituted for the product analysis. The transaction is assessed through the applicable rules and facts, rather than a label alone.

Situation 2. An unidentified government operator

An intermediary orders a system objectively designed for covert surveillance but refuses to name the public unit that will operate it. Its registration and financial standing are verified. Those facts do not resolve end use. The supplier requests minimum confirmation of the operator and legal basis, offering a confidential route for submitting information to the competent authority where appropriate.

The company places the relevant transfer on hold while the material inconsistency remains unresolved. Refusal to identify the user should not automatically be described as an already established breach of Article 5(2). Nevertheless, the company may lack a sufficient basis to proceed. Additional facts indicating intended repressive use require an assessment of notification duties and any applicable national suspicion rule.

The decision should explain what information is necessary and why. An indiscriminate demand for operational secrets may be neither useful nor proportionate. Confirmation of the actual user, its mandate and the applicable oversight arrangements may address the issue without identifying targets. If even that cannot be established, commercial pressure does not fill the evidential gap.

Situation 3. Remote activation in a different country

An authorised project covers access by a specified user in one country. Before commissioning, the integrator asks for the same module to be activated for another organisation in a different state. The physical server remains where it was. That does not make the change immaterial: the recipient and access map no longer matches the original dossier.

The supplier determines the actual transfer, the exporter and whether the authorisation covers it. Additional access is not granted before the issue is resolved. If the new organisation merely supplies a technical service without receiving the controlled object, access architecture should support that conclusion. The practical lesson is that equipment location cannot replace analysis of who receives software or technology.

The review should also identify whether the new organisation can delegate or extend access. A tightly bounded maintenance role differs from the power to create operational users or download controlled material. The conclusion should be based on implemented permissions and contractual authority, not merely the job title attached to the account.

Situation 4. A report involving a journalist

A researcher submits technically plausible material indicating that the product was used against a journalist. The evidence supports a likely connection to a tool family but does not yet establish the operator. The company preserves it, protects the reporter's identity, examines versions and compares the findings with lawfully available delivery information. Publicly accusing a particular customer would be premature.

If a potentially relevant operator is due to receive expanded functionality, the issue is immediately referred to the responsible decision-maker. A temporary hold on the expansion may be appropriate during review. A final court judgment should not be treated as the only permissible basis for preventive action. Equally, an initial technical hypothesis should not be represented as proven responsibility.

The company should avoid disclosing details that enable the operator to identify the complainant or destroy evidence. It may seek a narrowly framed explanation once the preservation and safety questions have been considered. If attribution remains unresolved, the closure record should state that limitation while explaining the risk-reduction measures actually taken.

Situation 5. A university and vulnerability disclosure

A laboratory intends to send information to an overseas developer so that a vulnerability can be fixed. The review identifies the materials, recipient and application of specific Annex I definitions or notes. If a relevant exclusion applies, the decision cites that basis. Academic status and public benefit do not, on their own, replace the legal analysis.

If the package also contains a different controlled module, that component is assessed separately. The procedure should permit lawful transmission of an eligible part without extending its treatment to the entire package without justification. Accurate classification protects research better than either extreme: a blanket ban on international exchange or an assumption that science is always exempt.

An urgent route can reduce the delay associated with this assessment without abandoning it. The laboratory supplies the minimum facts needed to distinguish the proposed disclosure from a broader technology transfer. Where uncertainty remains material, it seeks appropriate clarification rather than circulating sensitive material widely in search of informal reassurance.

Situation 6. A licence exists, but a participant's status changes

A supplier holds an EU licence but identifies a material change in a participant's status under an applicable restrictive regime before the next transfer. The sales team suggests relying on the old licence number. The responsible specialist checks the current restriction, its personal and substantive scope, exclusions and any need for a separate authorisation.

A historical sanctions announcement does not answer the current-status question; the applicable rule and entry must be checked. If an independent prohibition applies, a European dual-use licence does not remove it. The practical lesson is that an authorisation operates within its own legal regime rather than guaranteeing the lawfulness of every element of a transaction.

The delivery hold should be communicated accurately. If the obstacle is a current legal prohibition, management cannot waive it as a commercial risk. If it is an unresolved identification match, the company should seek evidence that resolves the match and record the outcome. Different reasons for stopping require different conditions for resuming.

19. The internal programme and accountability

Recommendation 2019/1318 describes core elements of an internal compliance programme: management commitment, organisational resources, training, transaction screening, audit, records and security. It was adopted under the predecessor Regulation 428/2009. This report therefore uses it as an organisational reference alongside current law, not as a replacement for Regulation 2021/821. [16]

In a small business, one employee may perform several functions, but conflicts of interest still need to be managed. A salesperson should not close a material issue in their own contract without appropriate review. Management can accept residual commercial risk within the law; it cannot waive a mandatory authorisation. Legal personnel identify requirements, engineering establishes characteristics and operations verifies delivery. Every decision needs an accountable owner.

Training should reflect work actually performed. Sales staff need to recognise a change of end user; engineers, a changed configuration; administrators, a new access grant; and finance staff, an unexplained mismatch between payer and contract. A generic sanctions lecture does not establish these skills. The consultation channel should deliver timely advice, or staff will be tempted to bypass a process that does not function within normal work.

Audit should sample completed transactions for consistency between authorisation and delivery, completeness of material information, handling of changes and implementation of restrictions. Reviewing prevented errors is also useful. The aim is to understand why a control worked or failed, not to increase the number of forms. Where a systemic defect is found, the process should be corrected rather than merely repairing an individual customer record.

ARGA proposes assessing the programme through verified end-user coverage, timely classification of new releases, quality of issue resolution and completion of corrective measures. The number of refusals is not, by itself, a success indicator: it may reflect diligent control or a poorly calibrated process. Absence of complaints also does not prove absence of harm if affected people do not know about the channel or cannot safely use it.

An effective programme should retain expertise when staff change. Product classification reasoning, authority correspondence and the limits of earlier approvals should be accessible to successors with the appropriate permissions. Otherwise, informal knowledge disappears and old approvals acquire an unjustified aura of permanence. A brief, current decision record is more useful than reliance on the memory of a former employee.

20. A decision record for an individual transfer

An export decision should connect legal assessment to approval of an actual action. ARGA proposes a concise decision record accompanying the technical and legal dossier. It is neither a substitute for a licence nor a mandatory governmental form. Its purpose is to give the delivery team a precise answer: what may be transferred now, to whom and subject to which conditions.

The record begins with the transaction identifier, the exporting legal entity, the product release and the proposed action. It then identifies applicable control grounds, authorisations and the end-use conclusion. Scope matters. “Delivery of software module version 4.2 to the identified operator” is testable; “the customer is approved” is too broad. The version number in this example is hypothetical and does not refer to an actual product.

A positive decision should state its boundaries and conditions. Access may be restricted to an identified recipient, an additional function may be excluded and an operator change may require reassessment. Where transfer depends on a condition being fulfilled, the access-management system should not treat the existence of the record itself as sufficient. The responsible person should separately confirm completion of that condition against the actual operation.

A negative decision also needs a precise basis. A direct prohibition, absence of a required licence, inability to establish the user and a corporate refusal because of residual risk are different grounds. The first two must be resolved under the applicable law; further information may resolve the third; the fourth requires identifying whether the policy permits reconsideration. The word “compliance” alone tells neither management nor the delivery team what should happen next.

Decision element	Illustrative content	Delivery check
Subject	A specified module and release	Match to the object transferred
Recipient	Legal entity and actual operator	Match to the access recipient
Basis	Classification and applicable authorisation	Validity and scope
Conditions	Functional or territorial limitation	Actual implementation
Duration	Date or material reassessment event	Continuing applicability
Accountability	Person authorised to approve	Verifiable approval

Consider a hypothetical project in which the supplier has identified the user and classified the module. The customer's statement describes operation by one public authority, but the access diagram includes two others. A sound decision record does not grant unconditional approval to the entire project. It identifies the unassessed access, requests the additional authorities' roles and determines whether the reviewed part can lawfully and technically be separated. If separation is artificial and still provides the same disputed capability, partial approval does not resolve the issue.

Further review may produce different outcomes. Confirmation that a second participant has only a narrowly technical role may resolve the concern. Discovery of another end user may require

changes to the dossier and authorisation. Facts indicating intended use for repression require examination under Article 5 and the relevant notification route. Preserving that sequence allows a later reviewer to see why the original answer changed.

The record should also identify who may implement the outcome. A legal approval with unresolved engineering conditions should not be interpreted as an instruction to activate the system immediately. Conversely, once the conditions are met, the process should avoid forcing staff to repeat the entire substantive assessment without reason. Linking the legal decision, technical confirmation and actual release creates a usable control rather than a disconnected collection of signatures.

21. Staged delivery and testing safeguards

Large projects often include demonstrations, trials, delivery, training and later updates. These stages do not necessarily have the same legal character or risk. ARGA proposes assessing the capability transferred at each stage and making progression depend on the relevant conditions. This is an organisational method, not a means of dividing a controlled operation into nominally insignificant fragments.

A trial may limit datasets, operator numbers and functions where the limitations are real and appropriate to the purpose. The label “pilot” does not create a licensing exemption. If a participant receives controlled software or technology, the applicable requirement is assessed before transfer. Demonstrating a system on synthetic data can reduce risk to people without automatically changing the export classification of the item itself.

Moving into operation requires comparison with the original dossier. The company should check whether the user, access location or configuration changed during the trial. Customer acceptance of the product must be distinguished from legal approval of delivery. A signed successful-test certificate supports a technical conclusion; it is not an export authorisation and does not establish the lawfulness of the intended surveillance.

Every mitigation measure should have a testable result. Where separation of duties is promised, the check should establish that a single operator does not retain the prohibited combination of permissions. Where onward transfer is restricted, the account-creation process and contractual chain should be examined. If independent audit is envisaged, its subject matter, available evidence and response to findings should be defined in advance. A tick indicating that an audit occurred does not establish that the risk fell.

Cost assessment should compare realistic alternatives. Removing a disputed module, changing the architecture and abandoning the transaction have different commercial and human-rights consequences. A proposed substitute must address the identified problem: a more expensive product with the same uncontrolled capability is not mitigation. Economic comparison can help select a workable option, but it cannot trade a mandatory prohibition for a higher expected profit.

Project closure also deserves attention. Expiry of a contract does not necessarily end access, invalidate keys or stop updates. The company should verify termination of the rights it is required or entitled to terminate, preserve necessary records and assess continuing security obligations. It should not promise deletion of every copy held by an autonomous user where that cannot be

verified. An accurate account of residual capabilities is needed when later support requests or new contracts arise.

A staged model is useful only if information passes between teams. Trial results may reveal a different operating environment; training may identify additional operators; support may disclose changed permissions. The procedure should carry those facts forward into the next decision instead of repeatedly relying on the original sales description. This is how implementation produces new knowledge relevant to control, rather than simply executing a conclusion fixed before the project began.

22. ARGA's position and implementation priorities

ARGA supports targeted controls that can prevent grave abuse while preserving legal certainty for legitimate activity. That requires consistent separation of technical classification, factual risk and the legal basis for restricting a transaction. Expanding a list without improving implementation does not resolve intermediary and update risks. Corporate review without a workable route to a competent authority likewise leaves material uncertainty.

ARGA proposes more anonymised guidance on borderline configurations, clearly distinguishing mandatory rules from recommended measures. This could reduce unjustified divergence without revealing sensitive user information. Public reporting should explain what is counted as an application, authorisation, refusal and actual export. The value of licences issued is not the value of goods actually exported, and the number of restrictions is not a direct measure of harm prevented.

For a company implementing the proposed model, the first thirty days should concentrate on products, releases, access channels and accountable personnel. The next stage should review the highest-risk existing relationships, update contractual mechanisms and establish the authority-engagement procedure. During the third month, the company can audit a sample of actual transfers and rehearse the handling of an abuse report. This is a suggested sequence, not a statutory ninety-day deadline.

Priority should reflect potential severity and the proximity of the next transfer. Producing an attractive policy while leaving tomorrow's activation unchecked would misallocate resources. Every identified gap should have an owner, a deadline and a verifiable result. Completion means a real change: access follows approval, a new release receives classification or a material report obtains a reasoned decision.

The system must allow review and correction. A responsible exporter should be able to show that a concern has been resolved or that the original information was mistaken. An affected person should have a safe way to report harm. The regulator should receive sufficient information for an independent decision. These conditions reinforce one another: sustainable control requires both effective restrictions and a reviewable procedure for applying them.

ARGA's practical standard is the ability to answer five questions: what capability was transferred; to whom; why the operation was permissible; what facts would change that decision; and how the organisation would learn of those facts. Where evidence supports the answers and delivery follows them, export control becomes a means of preventing harm. Where the answers exist only in declarations, even a formally complete licensing file leaves the central problem unresolved.

Sources and references

Legislation, official guidance and judicial materials. Accessed 28 September 2026. Numbers in square brackets refer to the sources below. Historical measures do not replace verification of current restrictions for a particular transaction.

- [1] Regulation (EU) 2021/821, 20 May 2021. Articles 2-5, 6-11, 15, 27; Annexes I and IV.
<https://eur-lex.europa.eu/eli/reg/2021/821/oj>
- [2] Commission Recommendation (EU) 2024/2659, 11 October 2024. Guidelines on the export of cyber-surveillance items under Article 5; Annex, sections 1-4. <https://eur-lex.europa.eu/eli/reco/2024/2659/oj>
- [3] Commission Delegated Regulation (EU) 2025/2003, 8 September 2025. Amendment of Annex I to Regulation 2021/821. https://eur-lex.europa.eu/eli/reg_del/2025/2003/oj
- [4] Commission Delegated Regulation (EU) 2026/1405, 26 June 2026. Corrections to certain language versions of Regulation 2021/821. https://eur-lex.europa.eu/eli/reg_del/2026/1405/oj
- [5] Direction générale des Entreprises. Service des biens à double usage (SBDU).
<https://www.entreprises.gouv.fr/service-des-biens-double-usage-sbdu>
- [6] Direction générale des Entreprises. Ai-je besoin d’une autorisation auprès du SBDU ? <https://www.entreprises.gouv.fr/espace-entreprises/s-informer-sur-la-reglementation/ai-je-besoin-dune-autorisation-aupres-du-sbdu>
- [7] Direction générale des Entreprises. Obtention d’une licence biens à double usage : qui fait la demande ? Quand faire la demande ? <https://www.entreprises.gouv.fr/espace-entreprises/realiser-mes-demarches/exporter-des-biens-double-usage/obtention-dune-licence>
- [8] ANSSI. Contrôle export. Regulatory guidance on cryptography and dual-use export controls. <https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/controles-reglementaires-cryptographie/controle-export/>
- [9] OHCHR. Guiding Principles on Business and Human Rights. 2011. Principles 17-22 and 29-31.
https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
- [10] BIS. Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities. November 2021. Historical administrative action. <https://www.bis.gov/press-release/commerce-adds-nso-group-other-foreign-companies-entity-list-malicious-cyber-activities>
- [11] US Department of the Treasury. Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium. 5 March 2024. Historical administrative action.
<https://home.treasury.gov/news/press-releases/jy2155>
- [12] European Parliament. Spyware: MEPs call for full investigations and safeguards to prevent abuse. 15 June 2023. Institutional account of the PEGA recommendations. <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse>
- [13] ECtHR, Grand Chamber. Big Brother Watch and Others v. the United Kingdom. Applications 58170/13, 62322/14 and 24960/15. Judgment, 25 May 2021; especially paragraphs 350-364, 377-382 and 448-450.
<https://hudoc.echr.coe.int/eng?i=001-210077>
- [14] Commission Recommendation (EU) 2021/1700, 15 September 2021. Internal compliance programmes for controls of research involving dual-use items. <https://eur-lex.europa.eu/eli/reco/2021/1700/oj>
- [15] Regulation (EU) 2016/679 (GDPR). Articles 5, 6, 25, 32 and Chapter V, subject to its scope of application. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [16] Commission Recommendation (EU) 2019/1318, 30 July 2019. Internal compliance programmes for dual-use trade controls under Regulation 428/2009. Organisational guidance read alongside current law.
<https://eur-lex.europa.eu/eli/reco/2019/1318/oj>