

TRADE CONTROLS POLICY

I. POLICY BACKGROUND

This Policy applies to Technoprobe S.p.A. and each of its subsidiaries (the **Group**). The Policy applies to everyone working for the Group regardless of location, role or level of seniority (collectively referred to herein as **Employees**). Any third parties acting on behalf of the Group, such as agents, consultants and partners, must also comply with the spirit of this Policy and all applicable laws and regulations.

Economic and financial sanctions, restrictive measures, trade embargoes or export control laws (**Trade Controls**) impose trade and financial restrictions on dealings with certain territories, entities and individuals or in certain goods and technology.

This Policy sets out requirements and procedures designed to ensure the Group's compliance with any applicable Trade Controls imposed by the United Nations (**UN**), European Union (**EU**) and the United States (**US**), or any other relevant jurisdiction and enforced by the respective competent authorities.

This Policy is maintained, implemented and updated at Group level by Technoprobe S.p.A.'s top management ("**Top Management**"), with the support of the Legal Department. At country level, country managers shall ensure appropriate implementation of the Policy, as well as handle any related issues that may arise with the support of the Legal Department. The Legal Department has an advisory role only, and all decisions shall be taken by Top Management.

Failure to abide by the requirements of this Policy could expose the Group to economic and reputational damage, and may result in criminal, administrative and civil liability to the Group, its affiliates or their respective directors, officers and employees. If you are ever unsure of how to react to a situation, you should always seek Group-level guidance from the Legal Department before you take action.

II. TRADE CONTROLS BACKGROUND

The Group and its Employees must generally comply with the Trade Controls imposed by the UN, EU and the US. For specific transactions and Group operations, the Trade Controls of certain

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

other countries will apply (and it will be the responsibility of the Group's country manager to monitor and ensure compliance with such Trade Controls).

EU Sanctions and Export Controls

EU sanctions target various activities involving specified third countries.¹ (EU sanctions incorporate all UN sanctions, but the EU also imposes unilateral measures.) The EU sanctions do not prohibit all business with a sanctioned country, but involve various types of measures: e.g. investment and trade bans, import and export restrictions on specified items, and restrictions in relation to certain designated individuals or entities (e.g. asset freezes). They also restrict certain activities involving targeted entities in particular industry sectors, including various sectors in Belarus and Russia ("**Sectoral Sanctions**").

The EU also imposes general export controls (which are based on multilateral export control principles) on various sensitive goods, software and technology that can be used for both military and civil purposes. The Group must determine whether export authorizations are necessary will require, for example, a careful and continuous product classification, a check on the countries of destination, an analysis of all the relevant regulations. In some countries, such export controls restrict any item supplied to a military customer. In addition, the EU imposes trade restrictions against Russia that cover certain semiconductor and microelectronic items. It will be important to monitor the Group's exposure to such general export controls and trade restrictions against specific countries as the Group's geographical footprint and product offering may expand (and as the restrictions continue to evolve).

Also relevant to the Group's activities are the EU asset freeze designations, as the Group cannot do business with such designated persons, directly or indirectly (including through companies that such designated persons own or control). The EU asset freeze designations can be found in a consolidated list.²

US Sanctions and Export Controls

In the US, the Office of Foreign Assets Control (**OFAC**) of the US Department of the Treasury has the primary responsibility for administrating, implementing, and enforcing economic sanctions. There are three general categories of OFAC sanctions: (1) country-based sanctions programs, (2) list-based sanctions programs (including Sectoral Sanctions), and (3) secondary sanctions that

¹ For a list of countries targeted by EU sanctions, see <https://www.sanctionsmap.eu/>.

² For the consolidated list of individuals and entities designated under the EU asset freeze, see <https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions>.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

mainly target non-US individuals and entities engaging in "sanctionable activity."³ (US sanctions incorporate UN sanctions, but the US also imposes unilateral measures.)

The comprehensive country-based programs impose broad sanctions restrictions in relation to the following countries/regions by way of example only:

- A. Cuba
- B. Iran
- C. North Korea
- D. Syria
- E. The Crimea region, as well as the Donetsk People's Republic and the Luhansk People's Republic (**Sanctioned Territories**).

OFAC publishes lists of designated parties, which include, among other lists, the Specially Designated Nationals and Blocked Persons List (**SDN List**) and the Foreign Sanctions Evaders List (**FSE List**) (collectively, **OFAC Lists**).⁴ In relation to Sectoral Sanctions, OFAC publishes the Sectoral Sanctions Identifications List (**SSI List**).

In addition, US export controls are particularly relevant to the Group. US export controls (including those administered by the US Department of Commerce's Bureau of Industry and Security (**BIS**) could in some cases apply to not just items located or manufactured in the United States, but also to certain foreign-manufactured products that contain US-origin content or derive from US technology). Some of the Group's products contain US-origin technology and are exported to several different countries. Accordingly, it is important for the Group to review and confirm for each relevant product that it is not caught by US export controls (or if it is, apply for a US export license). In addition, BIS maintains, under the Export Administration Regulations (**EAR**) a list of names of certain foreign persons that are subject to specific license requirements or additional restrictions for exports (**BIS Entity List**).⁵ In light of the geographical and product-related scope of the Group's activities, the Group must check that its customers and end-users are not subject to US export control related restrictions (and obtain any relevant US licenses if they are). Determining whether any authorizations under US export controls are needed will require careful consideration of any US content, use of US technology or software in the fabrication process, classification for US export control purposes, country of destination, end users, and end uses. For efficiency, a matrix should be maintained showing for each item of

³ For more information about OFAC's sanctions programs and relevant countries, see <https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>.

⁴ See <https://sanctionssearch.ofac.treas.gov/>.

⁵ To check customers and end-users against relevant lists such as the BIS Entity List, the Consolidated Screening List provided by the US government is a useful tool: <https://www.trade.gov/data-visualization/csl-search>.

hardware, software, or technology that is exported, the export classification, what export control regimes apply and what destinations require prior authorizations or licenses.

III. RESTRICTED PARTIES AND SECTORAL SANCTIONS PARTIES

The asset freeze, blocking or similar sanctions require the freezing or blocking of all property including funds belonging to, held, owned or controlled by designated parties. They also generally prohibit any dealing with or making funds, products or services available to, directly or indirectly, designated parties (e.g. through a third party). These designated parties are featured on the lists imposing asset freeze, blocking or similar restrictions (the **Sanctions Lists**), including those described and linked in Section 2.

Under this Policy, a **Restricted Party** means any individual or entity that is:

- listed on, or owned or controlled by⁶ a party listed on, the Sanctions Lists; or
- located or resident in, or incorporated under the laws of, the Sanctioned Territories.

In addition, as indicated above, the EU and US impose Sectoral Sanctions on certain listed entities in particular industry sectors (e.g. in Russia and Belarus), including in the financial, energy and defence sectors, and certain entities owned by, controlled or acting on behalf or at the direction of such listed entities (the **Sectoral Sanctioned Parties**). Such parties are listed on the US SSI List and various similar lists issued by the EU.

Sectoral Sanctions impose various specific measures, but do not prohibit all transactions with Sectoral Sanctioned Parties.

IV. OBLIGATIONS

Employees of the Group must conduct their work activities in compliance with this Policy and all applicable Trade Controls.

In particular, the Group and its Employees must **not**, directly or indirectly,

- engage in any dealings or facilitate any transactions involving any Restricted Parties. The Group must also not engage in any direct or indirect transactions involving Sectoral Sanctioned Parties, in violation of applicable Trade Controls; and
- provide or offer any item or technology to customers or other persons without any required export license or authorization.

The Group will seek to include appropriate obligations and conditions to promote compliance with applicable Trade Controls in all agreements with customers, suppliers, and any other counterparties (**Counterparties**).

⁶ "Owned or controlled" should be interpreted in accordance with applicable sanctions laws and guidance. For example, this means that under US sanctions any entity that is directly or indirectly owned 50 percent or more by one or more designated party is considered a Restricted Party. Under EU, UK and Norwegian sanctions, this means any entity that is directly or indirectly owned more than 50 percent by a designated party or otherwise controlled by a designated party (based on various factors indicating control) is considered a Restricted Party.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

V. TRADE CONTROLS COMPLIANCE PROCESS (COUNTERPARTIES)

Before any transaction takes place or any item is transferred, Employees must always establish relevant details by applying the "Know Your Customer" ("**KYC**") standard and assess if any Trade Controls may be applicable (including through screening of all Counterparties). If a direct or indirect Counterparty does not become known until after a transaction has commenced (e.g. because it is a new customer of the Group's direct counterparty), then the assessment must take place as soon as such Counterparty becomes known. Relevant KYC standard details include the identity of the Counterparty, the Counterparty's contact details, the identity of all other parties involved in the transaction (including all relevant customers of the Counterparty), and the end-use of any item or services to be supplied.

To the extent not already known based on existing business, the initial risk assessment must confirm:

- the **identity of the Counterparty** (including ownership),
- **where the Counterparty (and its parent company) is based**,
- the **end-use/destination of supplied products**, as applicable, and
- the **identity of any other parties** (including banks, to the extent possible) involved in the transaction.

For all Counterparties that you deal with, you must follow the sanctions and export control screening process established under Section 6 of this Policy. (This overall trade controls compliance process must also take into account any red flags, as per Section 7.)

You must suspend the transaction request and consult the Legal Department immediately if:

- i. you are requested to deal with a Restricted Party or Sectoral Sanctioned Party; or
- ii. you suspect that a Restricted Party or Sectoral Sanctions Party is involved in the transaction, directly or indirectly, or the transaction otherwise involves a red flag (see Section 7); or
- iii. the Counterparty is subject to specific license requirements or additional restrictions under EU or extra EU export controls (e.g. by being listed on the BIS Entity List).

If you become aware that any existing Counterparty is or has become the target of Trade Controls, then you must report this to the Legal Department.

The Legal Department will assess and escalate flagged transactions and parties as needed to Top Management. If Top Management approves a flagged transaction to go ahead after the required risk assessment, the Legal Department will then set out the conditions for the transaction, including any request for licenses or inclusion of sanctions/export control clauses in relevant contracts (for onward supply, etc.). You must also consult the Legal Department if the Group is asked to provide sanctions compliance undertakings in agreements.

If you become aware that any existing Counterparty is or has become a Restricted Party, a Sectoral Sanctioned Party, or has been added to the BIS Entity List, then you must report this to the Legal Department.

You must also report any known or suspected breaches of this Policy to the Legal Department that will investigate and assess the claims, as well as escalate them as needed to Top Management.

VI. SANCTIONS AND EXPORT CONTROL SCREENING

Sanctions Screening

To detect any Restricted Parties (including through links to Sanctioned Territories), Sectoral Sanctioned Parties, parties subject to license requirements under US export controls (see also Section 6.2) or transactions involving countries subject to sanctions beyond the Sanctioned Territories,⁷ the Group has established a process for screening the names, owners and contact details of all Counterparties against the relevant lists, e.g. of Sanctioned Territories, Sanctions Lists, lists of Sectoral Sanctioned Parties, and BIS Entity List, through an automated screening platform.

Screening must be performed at the initial point before any commercial relationship is established (and/or as soon as a direct or indirect Counterparty becomes known) and periodically thereafter at risk based intervals to take into account any related developments, as set out in Schedules 1 and 2.

The Group's country managers have overall responsibility of ensuring that required sanctions screening takes place according to this Policy at a local level. The Legal Department will provide support by ensuring that all relevant information is available for the screening process and by reviewing flagged cases and responding to queries. The Legal Department provides its assessment of flagged cases and escalate them to Top Management for approval. The ultimate decision as to whether or not to permit relevant transactions or activities lies with Top Management, namely with the Technoprobe S.p.A.'s Vice President or CEO.

Export Control Screening

As noted above, to detect any parties subject to specific license requirements or additional restrictions under EU or extra EU export controls, the Group has established a process for screening the names, owners and contact details of all Counterparties against the relevant lists, e.g. the BIS Entity List, through an automated screening platform.

If the Group decides to develop and supply new technology, software or services, the Legal Department, subject to approval by Top Management, is responsible for organizing and documenting checks as to whether such items are subject to export controls. This export control screening will take into account the precise specifications of any developed software and technology, such as any encryption functions and/or special design features to accommodate military end-users, especially if the item contains US-origin components or is derived from US

⁷ See Schedule 2.

technology. When necessary, the Group will request and obtain export classification decisions from the relevant Trade Controls Authority and/or seek advice from external counsel.

In addition, if a transaction is flagged as involving a country subject to sanctions beyond the Sanctioned Territories, the Group must perform specific screening of the products to be supplied against any relevant lists of goods subject to trade restrictions. The Legal Department will arrange for such product screening, including through the assistance of external counsel. Any hits will be reviewed by the Legal Department and escalated to Top Management for approval.

If employees suspects that an item and/or related technical information could be subject to applicable export controls (e.g. based on a reference in commercial documents for supplied items), the issue must be immediately reported to the Legal Department.

VII. RED FLAGS

The Group and its Employees are required to remain vigilant to ensure compliance with all applicable Trade Controls. They shall look out for any red flags that may indicate the direct or indirect involvement in a transaction of dual use items, a Restricted Party, Sectoral Sanctioned Party, party subject to specific license requirements or additional restrictions under EU, extra EU export controls or any other Trade Controls compliance concern.

To help in this assessment, see the non-exhaustive list of red flags in Schedule 3.

VIII. CONFLICT OF LAWS

In some cases, there may be a conflict between the local law of the Group Company and various other laws that apply to the Group. One such example is when US sanctions prohibit trade or dealings with a Restricted Party but European blocking statutes or anti-boycott laws require the Group not to comply with some of those sanctions laws. Another is when the sanctions assessment requires screening of an individual against foreign sanctions lists but the local data protection laws prohibit such screening. Any situation of conflict of laws must be reported to the Legal Department and carefully assessed on a case-by-case basis. Decisions in relation for conflict of laws shall be taken by Top Management, with support of the Legal Department.

IX. TRAINING

The Group will ensure that all relevant Employees receive training on Trade Controls and their compliance obligations under this Policy.

Training of all relevant Employees should take place on a periodic basis (preferably annually), according to the risk level of their role as determined by the Top Management.

X. RECORD RETENTION

The Group will comply with any retention requirements for all specific records compiled in accordance with applicable Trade Controls. All records related to transactions to which this

Policy applies (e.g. screening records) must be maintained for a minimum of five (5) years from the date of the last activity related to such transaction took place. Longer record retention periods may apply under the laws of a particular jurisdiction.

XI. MONITORING AND REVIEW

The Legal Department is responsible for monitoring developments in relation to this Policy and ensuring that the Policy is current and covers all relevant compliance risks.

Trade Controls, Restricted Parties, parties on the BIS Entity List, Sanctioned Territories, and Sectoral Sanctioned Parties change regularly and often on short notice. Therefore, this Policy will be revised if and when relevant legal and policy developments so require.

Any questions regarding this Policy or concerns about suspected breaches of this Policy should be directed to the Legal Department, which will review and provide their assessment prior to escalation to Top Management for final decision.

* * *

SCHEDULE 1: SCREENING PROCEDURE

The Group and responsible Employees (as identified by the Top Management) will screen all Counterparties using the following approach:

1. If the initial risk assessment of the contemplated transaction based on the Screening Instructions in Schedule 2 to this Policy indicates any sanctions or export control related information in relation to the sanctions-risk countries listed in the Schedule; Restricted Parties/Sectoral Sanctioned Parties/parties in the BIS Entity List based on specific screening; and/or any other "red flag" situation (see Schedule 3), this must be specially documented and flagged to the Legal Department.
2. To ensure appropriate screening, the responsible employee should ask the Counterparty to confirm its beneficial ownership (i.e. key shareholders), jurisdiction of incorporation or registration, and location(s) of its business operations. It may be appropriate to conduct searches of publicly available information to verify the information provided by the Counterparty, including to confirm the Counterparty's beneficial ownership.
3. The names and contact details of all Counterparties, and their key shareholders, must as a next step be screened against the lists of Sanctioned Territories and sanctions high-risk countries, the Sanctions Lists, BIS Entity List, the lists of Sectoral Sanctioned Parties and other relevant lists using an automated platform (see Schedule 2). Any positive hits, queries or concerns in relation to the screening results must be escalated to the Legal Department for review and appropriate action. If the screening results are negative (the screening did not produce any "hits" against applicable lists), then the transaction may proceed.
4. Whenever necessary (e.g. if the Counterparty's beneficial ownership is unclear), the Group should obtain a warranty or written confirmation from the Counterparty that it is not owned or controlled by a sanctioned party. (However, obtaining such a warranty or written confirmation is not a substitute for first conducting appropriate searches.)

Periodic Screening of Existing Counterparties

5. The names, contact details and beneficial owners of all existing Counterparties must be regularly updated and manually re-screened using the automated sanctions screening platform. The frequency of such updates and re-screening will depend on the risk profile of such Counterparties as determined by Top Management with support of the Legal Department, but will in any case take place at least annually. All positive hits or inquiries will be escalated to the Legal Department for review and appropriate action.
6. Screening must also be performed on any existing Counterparty if the Group or its Employees become aware of any new circumstances indicating that it should be flagged under Sections 5 and 7.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

* * *

SCHEDULE 2: SCREENING INSTRUCTIONS

STEP1: Please verify that you have the following information from the Counterparty (including in relation to any other parties involved in the transaction).

Counterparty Information

Full legal name of Counterparty, e.g. supplier (including type of entity)	
Other names used (including "doing business as" names, names used in the last 2 years or anticipated change in name)	
Date of incorporation (for entities)	
Address of incorporation	
Location(s) of any additional business operations, if involving the countries in Step 1	
Identification number (e.g. VAT identifier for entities)	
If you have been provided a copy of the entity's certificate of incorporation or similar document to confirm its company status and name, confirm that here.	

Beneficial Ownership Information for Counterparties:

Please provide the full legal name(s) and related information for all the direct and indirect shareholders that own a share of 25% or more of the Counterparty (and any lower shares if you have detected any indication that it is held by a Restricted Party or Sectoral Sanctioned Party).

Technoprobe S.p.A.
 Via Cavalieri di Vittorio Veneto, 2
 23870, Cernusco Lombardone (LC) - Italy
 www.technoprobe.com

Shareholder	Percentage of Ownership of Counterparty	Nationality / Jurisdiction of Incorporation and Address	Date of Birth (for Individuals)

Notes:

- If the shareholder (including ultimate beneficial owner in the shareholding structure) is a government or government entity, please include such shareholder too.
- Banks involved in each transaction which are incorporated/related to sanctioned countries and/or raise red flags must also be screened.

STEP 2: **Please check whether the contemplated transaction relates to any country listed below or any other “red flag” situation (see Schedule 3) that presents a risk from a Trade Controls perspective, i.e. as per Sections 5 and 7 of this Policy.**

Sanctioned Territories: Cuba, Iran, North Korea, Syria, Crimea Region of Ukraine, and the so-called Donetsk/Luhansk People’s Republics.

Sanctions high-risk countries: Ukraine, Russia and Belarus.

Other sanctions risk countries: Afghanistan, the Balkan region (e.g. Bosnia and Herzegovina, Kosovo, North Macedonia, Montenegro, Serbia), Central African Republic, China/Hong Kong, Democratic Republic of the Congo, Ethiopia, Iraq, Lebanon, Libya, Mali, Guinea, Guinea-Bissau, Myanmar (Burma), Nicaragua, Somalia, South Sudan, Sudan, Tunisia, Turkey, Venezuela, Yemen or Zimbabwe.⁸

- i. If the contemplated transaction involves a Sanctioned Territory or sanctions high-risk country, you may not proceed and must inform the Legal Department. Make sure you document all relevant information and present it to the Legal Department for further assessment, as required.***

⁸ The Legal Department, subject to approval by Top Management, will make sure this list of countries targeted by sanctions imposed by the EU and the US is up-to-date. When in doubt, please refer to the links included in Section 2 of this Policy.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

- ii. If the contemplated transaction involves any other sanctions risk country or a “red flag” situation (see Schedule 3), please move to Step 3 below.*
- iii. If the screening confirms that the contemplated transaction does not involve any country listed above or any “red flag” situation (see Schedule 3), you may proceed with the transaction. Make sure you confirm with the Legal Department as needed that the screening results have been properly documented.*

STEP 3: **Please screen the names of all relevant companies and individuals (e.g. shareholders) identified in Step 1 using the selected sanctions screening automated platform⁹:**

- i. Open the selected automated sanctions screening platform and enter the name of the company/individual you wish to screen.*
- ii. If there are any hits, you must not proceed with the transaction and/or activity; you must first inform the Legal Department and wait for further instruction.*
- iii. If there are no hits, you may proceed with the transaction under this Policy. Again, make sure you confirm with the Legal Department that the screening results have been properly documented.*

* * *

⁹ Top Management, with support of the Legal Department, shall selected an automated platform for sanctions screening.

SCHEDULE 3: RED FLAGS LIST

Although the red flag situations listed below may turn out to be entirely harmless from the Trade Controls perspective, it is strongly recommended to investigate such situations every time they occur. The list below is not exhaustive.

- The customer, especially if it is difficult to confirm its contact and beneficial ownership details, is asking for a different/strange invoicing/payment/shipment route.
- The customer, especially if it is difficult to confirm its contact and beneficial ownership details, requests shipment to or indicates substantial activities in an unusual location.
- A freight forwarding firm is listed as a supplied product's final destination.
- The customer, especially if it is difficult to confirm its contact and beneficial ownership details, is requesting that the delivery or service summary documents are addressed to another party.
- The address or the name of the customer is the same or very similar to that of a known Restricted Party or a party on the US Entity List.
- The customer orders spare parts or add-ons without having ordered a solution in which such parts or add-ons are normally used, where those spare parts or add-ons may be controlled or otherwise covered by sanctions or export controls.
- The customer is reluctant to provide certain information in writing, e.g. on the end use or the end user, on the ultimate destination, or on its beneficial ownership.
- The customer is related to, or somehow linked with, the military or defense industry, and is requesting specially designed products that are not part of standard solutions.
- The customer is new to you and your knowledge is limited, e.g. the customer does not have a website at all, or the Group website contains very limited information.
- The customer has little or no business background.

* * *