MARTURFOMPAK INTERNATIONAL	EXPORT CONTROLS AND SANCTIONS COMPLIANCE POLICY	Issued Date / Hazırlık Tarihi:	12.05.2026
		Revision Date / Revizyon Tarihi:	-
		Revision No / Revizyon No:	-
		Confidentiality level / Gizlilik Seviyesi:	L1
		Document No/Dokuman No	POL.23

1. OVERVIEW, PURPOSE AND SCOPE

We, Martur Fompak International, conduct business in an honest and ethical manner and have zero tolerance policy with regard to violations of laws and regulations with regard to Export Controls and Sanctions in all of our relationships and business dealings, where we operate.

With this Policy, we aim to declare our commitment to comply with applicable laws and regulations regarding Export Controls and Sanctions and to provide guidance for identifying and avoiding potential Export Controls and Sanctions risks, in order to preserve our integrity and reputation.

Therefore, we expect all our employees, including directors, Executive Committee members, and members of Board of Directors as well as all Business Partners, to comply with and act in line with this Policy and to always do business in accordance with our Global Code of Conduct.

The purpose of this Policy is to:

- Define our commitment to comply with all applicable Export Control and Sanctions Laws and Regulations;
- Establish principles and controls to prevent unauthorized Exports, Re-Exports, transfers, or disclosures, and
- Provide guidance to identify and manage Export Controls and Sanctions risks in our business operations.

2. DEFINITIONS

Dual-Use refer to Items, software, or technology that can be used for both civilian and military purposes or may have strategic applications. Dual-use items may also be subject to "catch-all" controls where there is knowledge or suspicion of prohibited End-Use or End-User, even if the item is not explicitly listed.
End-Use refers to the specific purpose and final application of the item or service, including the project requirements, the intended End-User, and the industry of destination.
End-User refers to the final customer, entity or individual that will receive the exported item or service.
Export refers to the shipment, transmission, transfer, or disclosure of goods, services, software, technology, or technical data from one country to another, including electronic transmissions and verbal disclosures.
Exports also include intangible transfers such as email, cloud access, VPN, remote desktop access, virtual meetings, or verbal technical assistance.
Export Administration Regulations (EAR) refers to U.S. regulations administered by the U.S. Department of Commerce that control the Export, re-Export, and transfer of certain goods, software, and technology, including Dual-Use items, for national security and foreign policy reasons.
Export Control refers to laws and regulations that allow, restrict, or prohibit the Export of an items or services, including but not limited to Regulation (EU) 2021/821. The applicable Export Control in each transaction will depend on the Item or Service, its destination, its End-Use and End-User.
Office of Foreign Assets Control (OFAC): refers to the U.S. authority responsible for administering and enforcing economic and trade Sanctions that restrict or prohibit transactions with certain countries, entities, or individuals.
Re-Export refers to the transfer of controlled items from one foreign country to another foreign country.
Restricted Party refers to any individual or entity subject to Sanctions, embargoes, denial lists, or similar restrictions issued by competent authorities.
Sanctions refer to trade, economic, or financial restrictions imposed by governments or international organizations against targeted countries, entities, or individuals.

3. GENERAL PRINCIPLES

We strictly comply with all applicable Export Controls and Sanctions Laws, including but not limited to:

- United Nations Sanctions regimes,
- European Union restrictive measures,
- U.S. Export Controls and Sanctions Laws and regulations (including EAR and OFAC),
- UK Export Controls and Sanctions Laws and Regulations, and
- Applicable local laws in the countries where we operate.

Regardless of local practices, commercial pressure, or competitive considerations, we do not authorize or tolerate any activity that violates Export Controls and Sanctions Laws. We recognize that violations may result in severe consequences, including:

- Loss or suspension of Export privileges,
- Significant administrative and criminal penalties,
- Seizure of goods,
- Reputational damage and
- Disciplinary measures against responsible individuals.

4. COMMITMENTS

4.1 Export Authorization and Licensing

All Exports, Re-Exports, and transfers of goods, software, technology, or technical data must be assessed to determine whether they involve items subject to Export Controls, including Dual-Use items, and whether an Export license or other authorization is required.
No controlled item may be exported or transferred without:

- Proper classification,
- Required approvals and licenses, where applicable, and/or
- Confirmation from the Legal and Compliance Team.

Business functions remain responsible for providing complete and accurate transaction data. Legal and Compliance validation does not transfer ownership of operational risk.

We do not permit or tolerate any attempt to bypass or evade Export licensing requirements, nor any false, inaccurate, or misleading Export-related information.

4.2 Sanctioned Countries, Entities and Individuals

We do not engage in business transactions that are prohibited or restricted by applicable Sanctions.
Prior to engaging in any transaction, appropriate screening must be conducted to ensure that:

- The destination country is not subject to comprehensive restrictions or embargoes, and
- The Business Partners, End Users, and other relevant parties are not Restricted Parties.

Employees have an obligation to make reasonable inquiries and escalate concerns where there are indications that screening results, End-Use, or End-User information may be inaccurate, incomplete, or misleading. Transactions involving sanctioned or high-risk jurisdictions require enhanced review and prior approval from the Legal and Compliance Team.

4.3 End-Use and End-User Controls

Employees and Business Partners must ensure that exported items are used solely for legitimate, declared, and lawful purposes.
We prohibit:

- Knowingly supporting prohibited End-Uses,
- Diversion of items to unauthorized End-Users, and
- Providing assistance where there is reason to believe items may be used in violation of Export Controls.

Any red flags or concerns regarding End-Use or End-Users must be escalated immediately.
Examples of red flags include refusal to provide End-Use statements, unusual routing, use of intermediaries without economic rationale, or involvement of high-risk jurisdictions.

4.4 Technology, Software and Information Transfers

The transfer or disclosure of controlled technology or technical data, including electronic transmission, remote access, or verbal communication, is subject to Export Controls regardless of the form or means by which such transfer occurs. This includes tangible and intangible transfers, such as electronic transmission, remote or cloud access, verbal communication, or any other form of making technology or technical data available.
Employees must not share controlled information by any means, with unauthorized persons and foreign persons within the same country, without prior assessment and approval.

4.5 Third Party Relationships

We may be held liable for Export Controls violations committed by Business Partners acting on our behalf. Therefore:

- A risk-based due diligence must be conducted before engaging Business Partners involved in international trade, and
- Contractual clauses requiring compliance with Export Controls and Sanctions Laws must be included where applicable.

No relationship may be established with Business Partners that carry unacceptable Export Controls or Sanctions risks.

4.6 Recordkeeping and Documentation

Accurate and complete records must be maintained for all Export-related transactions in accordance with applicable laws and internal procedures.
Records must:

- Reflect the true nature of transactions,
- Be retained for the period required under applicable laws and regulations, and in any event for no less than five (5) years,
- Be readily available for internal or regulatory review, and
- Be readily retrievable and sufficient to demonstrate compliance to external regulators and auditors.

Falsification or concealment of export-related information is strictly prohibited.

5. AUTHORITY AND RESPONSIBILITIES

All employees are responsible for complying with this Policy and Export Controls and Sanctions laws and regulations.
The Legal and Compliance Team oversees the implementation of this Policy, including:

- Providing guidance and approvals,
- Conducting training and awareness activities, and
- Monitoring compliance and investigating potential violations.

Employees who become aware of suspected or actual violations must report them promptly, in accordance with our Whistleblowing Policy, without fear of retaliation.

6. VIOLATIONS AND CONSEQUENCES

By this Policy, we actively prevent and prohibit such aforementioned or similar conduct. Our zero-tolerance principle means; if such a conduct does occur, we will look into and review every allegation of violation, initiate appropriate action in response. If there is a discrepancy between the local regulations, applicable in the countries where our company operates, and this Policy, subject to such practice not being a violation of the relevant local laws and regulations, the stricter of the two, supersedes. Violation of this Policy may result in significant disciplinary actions including dismissal and administrative, civil, and/or criminal liability under applicable laws. If this Policy is violated by Business Partners or any third parties, their contracts may be terminated.

This Policy will be periodically reviewed by the Legal and Compliance Team to ensure compliance with new or revised laws and regulations. Failure by management or governing bodies to ensure effective implementation of this Policy may result in administrative, civil, or criminal liability, in accordance with applicable legislation.