NETAŞ EXPORT CONTROL COMPLIANCE POLICY

Export Controls and Economic Sanctions

Published: 21.08.2019
Revised: 03.09.2024

COMPLIANCE DEPARTMENT

CONTENT

THE COMPANY'S COMMITMENT

This Policy is applicable for Netas's all domestic and international affiliates and subsidiaries. In issuing this Policy, Executive Committee Members and Board of Directors of Netaş Telekomünikasyon A.Ş. ("Netaş" or "the Company") affirm the Company's commitment to full compliance with all applicable export control and regulations, including but not limited to Turkish, EU and U.S. export controls and economic sanctions laws ("Export Control Laws"). U.S. export control and sanctions laws are in compliance with Turkish & EU export laws and regulations, and have a binding effect on the Company in export matters as long as there is no inconsistency. U.S. export control and sanctions laws can apply to Netaş' international and domestic business activities to the extent that they involve, directly or indirectly, such as through intermediary parties or third countries, the U.S. financial system or U.S. goods, software, technology, services, entities, or individuals. Netaş Executive Committee Members and Board of Directors of Netaş recognize that full compliance with all applicable Export Control Laws – and the terms of this Policy – is more important than any sale.

To ensure Netaş' commitment to compliance and to assist you as you pursue your day-to-day responsibilities, the Management of Netaş is responsible for establishing and maintaining the policies and procedures that are necessary to ensure that the Company maintains export compliance. Management is also responsible for training Netaş personnel and providing other compliance resources. The principles set forth in this Policy will be subject to further implementation in the form of internal compliance procedures to be developed by the Chief Compliance Officer (CCO), as described below.

Netaş expects every one of its employees, officers, directors, and agents or other third parties acting on Netaş' behalf, wherever located, to adhere to this Policy whenever taking any action on behalf of Netaş or related to Netaş' business. It is your responsibility to have a basic understanding of Export Control Laws as they apply to your duties; know the requirements of this Policy and Netaş compliance procedures where applicable to your duties; and seek appropriate guidance in a timely manner.

Personnel are encouraged to discuss any questions they have concerning Export Control Laws or this Policy with the Chief Compliance Officer of Netaş. Thank you in advance for your support and cooperation in this important effort.

Sinan DUMLU — CEO

Peng Ai Guang — Chairman of the Board

1- OVERVIEW OF THE POLICY AND RELEVANT LAWS

This Policy is designed to ensure that Netaş and its employees, directors, officers, and agents or other third parties acting on Netaş' behalf comply fully with all applicable Export Control Laws whenever taking any action on behalf of Netaş or related to Netaş' business. This Policy is designed to be published on the Company's internal webpage, and it will be maintained and updated whenever necessary.

Netaş's largest shareholder is ZTE Cooperatief U.A., a subsidiary of Zhongxing Telecommunication Equipment Corporation ("ZTE"). ZTE is subject to a U.S. Court-appointed Monitor (the "Monitor") and an ongoing compliance review by a Special Compliance Coordinator ("SCC") appointed by the U.S. Department of Commerce ("Commerce") pursuant to a settlement agreement with the U.S. Government. Due to ZTE's ownership interest in Netaş, Netaş is cooperating with ZTE's requirements under the agreements with the U.S. Government, including the compliance monitorship and review of the Monitor and SCC. Netaş expects all employees, affiliates, and subsidiaries to cooperate with all requests from the SCC and the Monitor and to implement actions recommended by the SCC and the Monitor to Netaş and its subsidiaries.

The primary U.S. laws and restrictions that may apply to Netaş (separately from and in addition to Turkish & EU laws and regulations applicable to Netaş) are:

- Economic sanctions, administered by the Office of Foreign Assets Control ("OFAC"), U.S. Department of the Treasury ("Treasury"). These rules impose restrictions on transactions involving targeted countries or regions, certain economic sectors, entities, and individuals when a U.S. nexus is present. Even if a transaction does not involve U.S. nexus, Netaş and other non-U.S. companies could face sanctions exposure under so-called "secondary sanctions" for engaging in certain business transactions targeted by U.S. sanctions.
- The Export Administration Regulations (the "EAR"), administered by the Bureau of Industry and Security ("BIS"), Department of Commerce. The EAR control the export, reexport, and transfer (in-country) of certain U.S.-origin goods, software, and technology (collectively "Items"), including foreign-made Items that incorporate a certain amount of controlled U.S.-origin content, such as parts, components and technology. A license issued by BIS may be required for the export, re-export, or transfer (in-country) of an Item if it is subject to the EAR.
- The International Traffic in Arms Regulations (the "ITAR"), administered by the Directorate of Defense Trade Controls ("DDTC"), U.S. Department of State ("State"). The ITAR severely restricts exports, re-exports, transfers, temporary imports, and brokering involving U.S.-origin defense articles, technical data, and defense services, including foreign-made Items that incorporate U.S.-origin defense articles and technical data. Transactions involving ITAR-controlled defense articles, technical data, or defense services that involve countries subject to a U.S. arms embargo, including China and Chinese nationals, are prohibited.

The laws and regulations described above can apply directly to non-U.S. companies (including Netaş) when a U.S. nexus is present and even in some cases, under secondary sanctions programs where no U.S. nexus is present. Critically, the ITAR and EAR apply to transactions by Netaş and other non-U.S. companies that involve the shipment, including in-country transfer, of U.S.-origin Items. There are severe criminal and civil penalties for violations of the ITAR and the EAR by companies and individuals. Any Netaş directors, officers, employees, or contractors found to be in violation of Export Control Laws, including the ITAR or the EAR, will be subject to disciplinary actions by the Company, up to and including termination.

Meanwhile, the regulations rendered by EU (Directorate-General for Trade (DG Trade)) and Turkish (Minister of Trade) Authorities shall also be considered when any business involved with these regions.

- Dual-Use Regulation (Regulation (EU) No 2021/821): Governs the export, transfer, brokering, and transit of dual-use items, which can be used for both civilian and military purposes. This regulation is central to the EU's export control regime.

- Sanctions Regulations (e.g., Regulation (EU) No 833/2014): These regulations impose restrictions on exports to specific countries or entities based on the EU's Common Foreign and Security Policy (CFSP). They cover embargoes on arms, restrictions on certain goods and services, and other measures.

- Regulation (EU) 2019/125: Controls the export of goods that could be used for capital punishment, torture, or other cruel, inhuman, or degrading treatment.

- List Related to Warfare Tools and Equipment, Weapons, Ammunitions and Their Parts, Military Explosive Material and Their Technologies" (often referred to as the "5201 List").

2- CHIEF COMPLIANCE OFFICER

As part of its overall compliance plan, the Company has appointed a Chief Compliance Officer who is also the Export Control Point of Contact. The CCO will serve as the in-house coordinator for all sanctions and export controls-related matters. The CCO is responsible for overseeing all export compliance functions, such as screening proposed transactions against the list of sanctioned countries and persons. The CCO is also responsible for staying informed on trade controls matters, including updating this Policy as necessary. Questions concerning export controls and the Company's policies and procedures with respect to exports should be addressed to the CCO, Börgehan Köksal, at bkoksal@netas.com.tr or at +90 216 522 2525.

3- ECONOMIC SANCTIONS

The U.S. Government maintains laws and regulations that prohibit business activities involving certain entities, individuals, or countries (including their nationals wherever situated). These controls are far-reaching and can apply not only to U.S. companies, but also to U.S. persons living and acting outside the United States and to foreign entities that are dealing in U.S.-origin Items or

U.S. dollars, or engaging in transactions subject to U.S. secondary sanctions. As a matter of policy and to ensure full protection to itself and to U.S. entities and persons that are involved with the Company, Netaş conducts itself in a manner that complies with all U.S. economic sanctions, even when there is no U.S. nexus.

- **Comprehensively Sanctioned Countries/Regions**

The following countries/regions are subject to comprehensive sanctions (collectively referred to as "Restricted Regions"), meaning that virtually any transaction involving these countries/regions is prohibited[1]:

- Crimea, Luhansk and Donetsk Regions of Ukraine
- Cuba
- Iran
- North Korea
- Syria

To ensure full compliance with these rules, it is the policy of Netaş to do no business, directly or indirectly, with, or to benefit, any individuals, persons or entities organized or located in Crimea region, Cuba, Iran, North Korea, or Syria. These prohibitions include the following:

- Participating in, providing business approvals, facilitating, assisting, advising on, or supporting any transactions involving these countries or with any entity known to be owned, controlled, or organized in Restricted Regions.
- Exporting, re-exporting, or transferring Items to any destination if Netaş has any reason to believe such shipment is ultimately intended for a Restricted Region.
- Providing any service, including technical support, repairs, returns, or warranty services to persons or entities in Restricted regions.
- Importing Items from a Restricted Region.
- Brokering, arranging or performing any contract (including a contract for the sale of goods or services) if Netaş has reason to know it will ultimately benefit a Restricted Region. This includes contracts with persons anywhere in the world.
- Engaging in investments or financial transactions, including payments to or from, involving Restricted Regions.
- Approving or facilitating any transaction or activity involving a Restricted Region.

- **Targeted Sanctions**

U.S. law also prohibits U.S. persons from engaging in any business transactions with a broad range of individuals or entities designated as terrorist supporters, narco-traffickers, or for engaging in other activities condemned by the United States. OFAC maintains targeted sanctions programs

[1] On January 14, 2021 the Bureau of Industry and Security (BIS) of the U.S. Ministry of Commerce cancelled Anti-terrorism controls on Sudan, and revised EAR.

against a number of countries/regions, imposing restrictions on certain activities and designated persons.

4- RESTRICTED PARTIES

As noted, OFAC maintains several lists of sanctioned persons for which certain (or all) transactions are prohibited, including:

- **the List of Specially Designated Nationals and Blocked Persons ("SDNs"):** This list identifies entities, individuals, and organizations with whom transactions involving any U.S. nexus, including U.S. persons, U.S. items, and U.S. dollars, are generally prohibited. Secondary sanctions may apply to activities with such persons and entities even if no U.S. nexus is involved. To ensure full compliance with these far-reaching rules, this Policy prohibits any direct or indirect transactions or business relationships with any SDN on the Company's behalf.
- **the Sectoral Sanctions Identifications List ("SSIL"):** This list identifies companies in the financial, energy, and defense sections of the Russian economy and prohibits certain types of activities with these entities involving a U.S. nexus.

Only activities in full compliance and approved by the CCO are permitted with these entities.

- **the List of Foreign Sanctions Evaders ("FSEs"):** This is a list of non-U.S. individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions and non-U.S. persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions. Transactions by U.S. persons or within the United States involving such individuals are prohibited.

In addition, BIS and DDTC maintain their own lists of persons with whom transactions are restricted, including:

- **BIS's Entity List:** This is a list of non-U.S. parties that are prohibited from receiving some or all items subject to the EAR unless the exporter secures a license from BIS. Generally, license exceptions are unavailable. Only activities in full compliance and approved by the CCO are permitted with these parties.
- **BIS's Denied Persons List:** This is a list of individuals and entities that have been denied export privileges. Any dealings with a party on this list that violate the terms of its denial order are prohibited. Only activities in full compliance and approved by the CCO are permitted with these individuals and entities.
- **BIS's Unverified List:** This list identifies parties that are ineligible to receive items subject to the EAR by means of a license or license exception, and exporters must file records for all exports to parties on this list and obtain specific statements from parties. Only activities in full compliance and approved by the CCO are permitted with these parties.
- **DDTC's Debarred List:** This list identifies entities and individuals that are prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services. Only activities in full compliance and approved by the CCO are permitted with these parties.

These lists above are referred to collectively in this policy as “Restricted Party Lists”. Transactions involving Restricted Parties may be prohibited, and a case-by-case analysis by the CCO is required prior to any dealings that may involve a Restricted Party.

The CCO shall be responsible for implementing and maintaining appropriate procedures for screening transactions and counter-parties against Restricted Party Lists, and all personnel shall comply with those procedures.

5- EXPORT CONTROLS ON U.S.-ORIGIN COMMERCIAL AND DUAL USE ITEMS

The EAR regulates exports, re-exports, and transfers of commercial and “dual use” (i.e., having both civilian and military applications) Items that are U.S.-origin or that are foreign-made and incorporate a certain amount of controlled U.S.-origin content.

Although Netaş has no U.S. operations, it does, and may in the future, receive, procure, and use Items subject to the EAR. Items subject to the EAR may include parts, components, equipment, resale products, software, source code, or technology received or procured by Netaş. When Netaş engages in the procurement of Items subject to the EAR, it must confirm the ECCN of the Items, assess any controls imposed upon such Items, and, to the extent the Items are subject to any licensing requirements, ensure that any transactions in which it engages involving such Items take place in full compliance with the terms of any licenses received by the vendor or by Netaş itself. Transactions that may be subject to licensing conditions apply not only to exports and re-exports, but also to transfers of such Items within a single country (e.g., Turkey) where the end-use or end-user of the Item changes, even if to an affiliated company.

Commodity Classification and Licensing

Items that are controlled and that may require a license from BIS are generally set forth on the EAR’s Commerce Control List (“CCL”). The CCL sets forth Export Control Classification Numbers (“ECCNs”) that categorize items and may require authorization from BIS for export, reexport, or transfer (in-country), depending on the (i) nature of the Items and their jurisdiction/classification under the EAR; (ii) country of destination; (iii) intended end-user; and (iv) intended end-use.

For instance, ECCN 5A002 controls certain information security systems, equipment, and components, in part based upon where they are to be shipped. Prior to engaging in a transaction that would involve exports, re-exports, or transfers of such Items that are subject to the EAR, Netaş must ensure that all appropriate licenses have been received, an appropriate license exception applies, or no license is required.

License Exceptions

The EAR sets forth certain License Exceptions that allow controlled items to be exported, re-exported, or transferred without a specific export license. Each License Exception has specific defined requirements and a License Exception can only be used if ALL conditions and requirements have been met.

For example, License Exception ENC authorizes the export, re-export or transfer of controlled encryption items to certain countries, end-users and end-uses, and sets forth detailed requirements for such transactions. See "Restricted Encryption Items" below.

Items Subject to the EAR

Items not on the CCL remain subject to the EAR and are classified in the "basket" category known as "EAR99". These Items can be exported without restriction around the world, except to Restricted Regions, to prohibited end-users (e.g., certain Restricted Parties), or for prohibited enduses, including missiles, nuclear, chemical, and biological weapons related activities.

Encyrption Items

Items subject to the EAR that incorporate or call upon encryption or decryption functionalities are subject to export control restrictions that vary depending on the nature of the encryption functionality employed and the non-US end-user of the encryption Item through an export, re-export, or transfer. Depending on the type of encryption, a specific export license may be required to export, re-export, or transfer the encryption Item or the item may be exported, reexported or transferred without a license pursuant to License Exception ENC. License Exception ENC authorizes the export of certain encryption Items depending on the destination country and the nature of the end-user. Netaş employees must ensure that any transfers, exports, re-exports of Items with encryption functionality that are subject to the EAR are consistent with the terms of a specific license or License Exception ENC, or do not require a license.

Certain encryption Items, known as "Restricted Encryption Items", may not be exported, re-exported, or transferred to certain government end-users. Under the EAR, "government end users" are defined as any foreign central, regional or local government department, agency, or other entity performing governmental functions; including governmental research institutions, governmental corporations or their separate business units (as defined in part 772 of the EAR) which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and international governmental organizations.

With regard to encryption Items and License Exception ENC, certain encryption items may be exported to government end-users without a license that are excluded from the definition, including utilities, public civilian hospitals, telecommunications companies and internet services providers, and financial institutions. By contrast, certain government institutions are

classified as “more sensitive government end users,” including national laboratories, currency and monetary authorities, intelligence and defense agencies, and information technology agencies.

When engaging with a potential government end-user, Netaş employees are required to first consult with the CCO before exporting, re-exporting, transferring, or disclosing any encryption Items.

600 Series Items

Certain defense articles formerly controlled under the ITAR are controlled under the EAR as “600 Series” Items. This change in control and classification was implemented to establish more flexible controls for Items exported to certain countries. However, licensing requirements for items classified in the “600 Series” will generally require a license for export, re-export, deemed re-exports, or transfers. Moreover, “600 Series” Items may not be exported to countries subject to a U.S. arms embargo, such as China. Accordingly, Netaş policies applicable to ITAR-controlled Items (described below) are applicable to all Items classified under the “600 Series”.

Deemed Exports and Re-Exports of Controlled Technology or Source Code

Under the EAR, the release of controlled technology or source code to a foreign person in the United States is considered to be a “deemed” export or re-export (“Deemed Export”) to the home country or countries of the foreign person. A Deemed Re-Export can occur, when controlled technology is shared in a foreign country (e.g., Turkey) with a third country national (e.g., a Chinese national) employee, contractor, visitor, or other party working at a company facility. The technology is “deemed” to have been re-exported to that person’s home country. Deemed Exports and Re-Exports are subject to the same legal restrictions and Netaş policies as all other exports, re-exports, and transfers.

6- EXPORT CONTROLS ON U.S.-ORIGIN DEFENSE ARTICLES, TECHNICAL DATA, AND DEFENSE SERVICES

Exports, re-exports, transfers, temporary imports, brokering, and services involving U.S.origin defense articles and technical data, including foreign-made Items that incorporate U.S.origin defense articles and technical data, are controlled by DDTC under the ITAR. Such Items are identified on the ITAR’s U.S. Munitions List (“USML”), which has 21 categories, including, but not limited to, firearms, weapons systems, and military aircraft; personal protective equipment; military vessels and vehicles; missiles, rockets, and bombs and bomb parts and components, as well as items specifically modified or customized for defense purposes, and certain test equipment. Transactions with non-U.S. companies involving ITAR-controlled defense articles and technical data are generally prohibited without a license from DDTC.

Prior to receiving, accepting, procuring, using, or otherwise handling any ITAR-controlled Items, technical data, or services, employees must seek immediate guidance from the Chief Compliance Officer and not proceed until such guidance is received.

Commodity Jurisdiction

In general, a particular Item is subject to controls under either the ITAR or the EAR. Thus, the critical first step in export controls compliance is determining whether a particular Item falls under the ITAR's USML, which is a more restrictive set of regulations than the EAR. Companies may seek a formal determination, called a "commodity jurisdiction request", from DDTC on whether an Item is subject to the ITAR.

Defense Articles and Defense Services

In general, defense articles include any Items, including technical data and defense services, identified on the USML or specifically designated by DDTC as a defense article or service based on a determination that it (i) provides the equivalent performance capabilities of an Item on the USML; or (ii) provides a critical military or intelligence advantage such that it warrants control under the ITAR.

The definition of defense article controlled under the ITAR also includes parts and components that are specially designed, developed, modified, configured, or adapted for use with defense article and foreign-made defense articles incorporating ITAR-controlled Items. Further, the ITAR controls the provision of defense services, which is defined to include, inter alia, furnishing technical data or providing assistance (including training) to the development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles.

- **Hardware**

Of particular note, USML Category XI(a)(5) lists as defense articles electronic equipment and systems such as command, control, and communications; command control, communications, and computers; command, control, communications, computers, intelligence, surveillance, and reconnaissance; and identification systems or equipment that are specially designed to integrate, incorporate, network, or employ certain other defense articles or that implement active or passive electronic counter-countermeasure ("ECCM") used to counter acts of communication disruption.

Such defense articles would require a license prior to engaging in exports, re-exports, transfers, or services that would involve them.

- **Technical Data and Software**

As noted, the definition of controlled defense article includes technical data, which is (i) any information (classified or unclassified) required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles as well as software directly related to defense articles; (ii) any classified information

relating to defense articles and defense services; and (iii) software that is directly related to defense articles. Technical data can include information in the form of blueprints, drawings, photographs, plans, instructions, and documentation.

Restricted Transactions

The ITAR prohibits transactions involving defense articles without a license from DDTC. These transactions include, but are not limited to:

- Sending or taking a defense article out of the United States in any manner;
- Transferring registration, control or ownership to a foreign person of any U.S.-origin aircraft, vessel, or satellite covered by the USML, whether in the United States or abroad;
- Disclosing (including oral or visual disclosure) or transferring ITAR-controlled technical data to a non-U.S. person, whether in the United States or abroad;
- Performance by a U.S. person of a defense service on behalf of, or for the benefit of, a nonU.S. person, whether in the United States or abroad; and
- Engaging in the export, re-export, or transfer (in-country) of a procured ITAR-controlled defense article. This includes engaging in such transactions involving ITAR-controlled defense articles procured from a vendor under a valid license. Transactions after the receipt of the defense article that are not specifically authorized by the license, including transfers to third parties within Turkey, are prohibited.

Licensing

Export licensing policies under the ITAR are more restrictive than under the Commerce Department's EAR. Licensing decisions are based on an inter-agency review process that includes substantial input from the U.S. Department of Defense. Any Netaş transactions or movements of equipment that might involve an ITAR-controlled Item must strictly adhere to all licensing conditions and the restrictions imposed by the ITAR.

As noted, transactions involving ITAR-controlled defense articles and technical data, including re-exports and in-country transfers, generally require a license from DDTC. Netaş employees may not participate in transactions involving Items controlled under the ITAR without appropriate authorization. Critically, even if a defense article was procured by Netaş or another party lawfully pursuant to a license issued by DDTC, additional exports, re-exports, and transfers of that Item may need to be further licensed if such transactions were not included in the original authorization. As a result, it is essential that Netaş employees ensure that every transaction involving ITAR-controlled defense articles is specifically authorized under a license issued by DDTC or does not otherwise require such a license.

A license issued by DDTC may include conditions or provisos. In ensuring compliance with the terms of a license, Netaş employees must be certain that all conditions and provisions included in a license are strictly followed, including terms of non-disclosure set out in any NonDisclosure Agreements that Netaş is asked to execute as a condition of receipt of such Items.

Proscribed Countries and Territories

DDTC maintains a list of countries subject to arms embargo or with which transactions involving ITAR-controlled transactions are generally proscribed and for which a license will generally be denied. This list, set forth at https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126, includes a number of countries. Netaş maintains a strict policy to refrain from any business involving ITAR-controlled Items with such countries or territories.

Technology Control Plan

To the extent Netaş is approved as a recipient in a DDTC export license or authorization, certain non-Turkish employees of Netaş may not be authorized to access or work with defense articles or technical data that Netaş acquired under the license or authorization. In order to ensure compliance with such restrictions on retransfers of such Items, Netaş will need to implement a Technology Control Plan ("TCP") restricting access to such Items by certain personnel. A TCP explains what restrictions apply to particular individuals and measures that will be observed to ensure Netaş personnel do not inadvertently violate restrictions on the export or deemed export of controlled Items. All Netaş personnel, including the individuals involved and any personnel working with those individuals are required to comply with the terms of the TCP.

7- COMPLIANCE TRAININGS

The CCO will coordinate and conduct periodic export compliance training and reviews to ensure that all Netaş employees understand the rules set forth in this Policy and that all compliance procedures issued pursuant to this Policy are being effectively implemented. The CCO and other Netaş management are responsible for identifying the personnel required to participate in this training. Participation in periodic export control compliance training is mandatory for all Netaş employees, including senior management, sales, legal, supply chain and engineering personnel. Netaş personnel that work in or have access to the R&D labs are required to participate in periodic ITAR compliance training and their attendance shall be documented. Participation in training will be documented through training logs and regular certification by Netaş personnel of participation in training and their understanding of the Policy.

8- SELF ASSESSMENTS AND AUDITS

The CCO will, on an annual basis, conduct audits of Netaş business units and divisions and utilize a checklist of items during their audits to identify potential export compliance risk factors as part of Netaş' regular compliance audit process. The scope of such audits will generally cover more than just export compliance matters touched on in this Policy, but checklists and training will be used in conjunction with the wider audits to flag any export compliance matters needing attention and/or remediation. The CCO will document the results of such audits and implement measures to remedy any risk factors identified. This audit function is being implemented in connection with the sales and operations process and will be applied to other parts of the Company as and when required.

9- QUESTIONS AND CONTACTS

If you have any questions concerning this Policy or the legality of a particular transaction, please contact Chief Compliance Officer Borgehan Koksal, at bkoksal@netas.com.tr or at +90 216 522 2525. Or, please contact with Compliance Department via compliance@netas.com.tr.

All employees and contractors are required to report any potential export compliance issues or violations. Any reports of potential violations may be made to the Netaş Chief Compliance Officer, and under no circumstances will any Netaş employee or contractor be subject to retaliatory action for reporting in good faith an actual or suspected violation.

- External reporting mechanism,
  - Website: http://www.tip-offs.com.cn/ZTE
  - E-Mail: ZTEWhistleblowing@tip-offs.com.cn
  - Hotline: +8621-3313-8584

- Internal reporting mechanism,
  - Whistleblowing Channel: https://netas.com.tr/netas-ihbar-hatti
  - E-mail: compliance@netas.com.tr