

**Distribution:** General

**Date:** April 28, 2026

**Original Language:** Turkish

## ÖZALTIN HOLDING A.Ş.

### ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND COUNTER-PROLIFERATION FINANCING POLICY

#### 1. PURPOSE AND SCOPE

The purpose of this Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing Policy (“Policy”) is to establish the principles and rules that must be considered to ensure compliance with the obligations of Özaltın Holding A.Ş. and its group companies (“Company”) regarding the prevention of money laundering, terrorism, and the financing of weapons of mass destruction.

All employees and managers of the Company are obligated to act in accordance with this Policy, which is an integral part of the Company’s Code of Ethical Conduct. Furthermore, the Company expects all Business Partners to act in accordance with this Policy to the extent applicable to the relevant party and/or transaction, and takes the necessary steps to ensure this.

#### 2. DEFINITIONS

The term “**Government/Public Official**” refers to any person who participates in the conduct of a public activity through appointment or election, or in any other manner, on a permanent, temporary, or interim basis, including but not limited to the following:

- Individuals employed by any public institution or public economic enterprise within the country or in a foreign country,
- Employees of any political party located within the country or in a foreign country, and all political candidates,
- Individuals holding positions in any legislative, executive, or judicial body within the country or in a foreign country,
- Judges, jurors, or other judicial officials serving in national, international, or foreign state courts,
- Officials or representatives working in national or international parliaments;
- Arbitrators serving in arbitration proceedings initiated to resolve a legal dispute.

“**FATF (Financial Action Task Force)**” is an international organization established in 1989 to develop policies and set standards to combat a range of crimes, including money laundering,

human and drug trafficking, terrorism, and the financing of the proliferation of Weapons of Mass Destruction.

**“Ultimate Beneficial Owner (UBO)”** refers to the natural person or persons who ultimately control a legal entity or an unincorporated entity, or who exercise ultimate influence over such entities.

**“Business Partners”** include suppliers, customers, contractors, and any representatives, subcontractors, consultants, and other third parties with whom the Company has a business relationship, as well as the employees and representatives of such entities.

**“Politically Exposed Person (PEP)”<sup>1</sup>**, refers to high-ranking individuals who, currently or in the past, domestically or in a foreign country, have been entrusted with a significant public office through election or appointment; members of the board of directors, senior executives, and executive assistants of international organizations; other individuals performing equivalent roles; senior politicians; senior officials of political parties; senior judicial, administrative, or military officials, as well as senior executives of public economic enterprises, and the spouses, first-degree relatives (parents and children), and close associates of all such persons.

**“Weapons of Mass Destruction”** refers to nuclear, chemical, and biological weapons, as well as ballistic missile programs, as defined under United Nations Security Council resolutions

**“Özaltın Holding”** refers to Özaltın Holding A.Ş.

**“Proceeds of Crime”** refers to the value of assets derived from criminal activity.

**“Money Laundering”** refers to the integration of proceeds from illegal activities into the financial system as if they were obtained legally; in other words, it is the concealment of the fact that these proceeds were derived from illegal activities.

**“Company”** refers to Özaltın Holding A.Ş., Özaltın Construction, Trade, and Industry A.Ş., Özaltın Hotel Operations A.Ş., Özaltın Greenhouse and Trade A.Ş., Özaltın Energy Production and Construction A.Ş., Zenit Mining Industry and Trade A.Ş., Enova Electricity Wholesale Sales Inc., Enova Energy Production Inc., Özaltın Import Export and Construction Inc., Özaltın Mining Trade and Industry Inc., Özaltın 2 Energy Investments Inc., Özaltın 3 Energy Investments Inc., Nova Investment S.A., and Pontid Mining Industry and Trade Inc.

**“Misconduct”** refers to any intentional act or omission intended to deceive others for the purpose of obtaining unjust enrichment or causing harm. This includes the misuse of the company’s resources or assets by an individual for the purpose of securing personal or corporate gain.

---

<sup>1</sup> <https://www.fatf-gafi.org/documents/documents/peps-r12-r22.html>

“**Financing of Terrorism**” refers to activities that provide material support to terrorist individuals, groups, organizations, or supporters of terrorism.

### 3. GENERAL PRINCIPLES

To manage the risks it may face regarding Money Laundering, the financing of terrorism, and the proliferation of Weapons of Mass Destruction (“**AML-CFT**”<sup>2</sup>), the Company applies relevant legislation in all its transactions by leveraging the work and guidance of leading international organizations in this field.

If Company employees engage in, assist in, or participate in any misconduct that would facilitate money laundering or the financing of terrorism and the proliferation of Weapons of Mass Destruction, either directly or indirectly, create a risk of unlawfully concealing the nature of such transactions, or result in criminal proceeds; the Company will not tolerate employees engaging in, aiding, or participating in any such misconduct. This prohibition also covers misconduct committed by Business Partners acting on behalf of employees or the Company, even if such acts are for the benefit of the Company or third parties.

In this context, in all transactions in which the Company is a party,

- necessary measures must be taken to effectively manage risks related to AML-CFT,
- KYC procedures must be conducted in compliance with regulations and on a regular basis to identify the identities of Business Partners and customers, and an Enhanced Due Diligence (“EDD”)<sup>3</sup> must be performed when necessary,
- In the event of the detection of unusual or suspicious activities, the transaction must be thoroughly investigated, and if necessary, immediately suspended, and the relevant authorities must be notified<sup>4</sup>.

### 4. IMPLEMENTATION OF THE POLICY

#### 4.1. Know Your Business Partner

Business and operational units must, prior to establishing a business relationship with a new Business Partner, identify potential risks related to AML-CFT and ensure that the relevant party is not a Sanctioned Entity, and by obtaining all necessary commitments in accordance with the applicable data protection legislation in the countries where the Company operates, are responsible for conducting a Due Diligence Study using a screening tool. The following points are taken into consideration to ensure this study is effectively carried out<sup>5</sup>.

---

<sup>2</sup> AML-CFT: “Anti-Money Laundering / Countering the Financing of Terrorism”

<sup>3</sup> For details, please refer to the Company Supply Chain Compliance Policy and the Company Sanctions and Export Controls Policy.

<sup>4</sup> Legal authorities are informed by a lawyer assigned to the Legal and Compliance Department or by an external lawyer appointed for this purpose.

<sup>5</sup> Primary responsibility for the listed processes lies with the business and operational units.

The tax office and numbers of Business Partners, as well as the valid identification and address information of their authorized representatives and (if applicable) shareholders, as recognized by the relevant authorities, are identified. The information obtained is verified without fail if required under applicable legislation or if there are doubts regarding its reliability and validity. Additionally, investigations are conducted to identify Ultimate Beneficial Owners (UBOs) in accordance with the law. Detailed information is obtained regarding the profession, the industry in which the business operates, the sector from which income is derived, the duration of operations in that sector, and the commercial history.

- Information is obtained regarding the nature and level of activity of the current and potential business relationship with the company.
- Information is obtained regarding the countries and regions where the declared business sector is conducted<sup>6</sup>.
- When establishing and maintaining a business relationship, a screening tool is used to regularly check national and international sanctions lists and monitor negative media reports to determine whether the Business Partner or UBO has been involved in financial crimes or other serious offenses, including fraud, and to identify potential risks related to sanctions and export control regulations.
- Whether the Business Partner or UBO is a Public Official or a Person with Public or Political Influence is verified through internet and media searches and other databases.
- All information, documents, and records obtained are periodically updated and retained for a minimum of 5 years from the date of the last transaction.

If, as a result of the Due Diligence Study conducted by taking all obtained information into account, any adverse finding, reasonable suspicion, or potential non-compliance with this Policy or applicable legislation is identified, the matter is immediately reported to the Legal and Compliance Department. The Legal and Compliance Department may decide to suspend the transaction after conducting the necessary assessment, or may request an Enhanced Due Diligence (EDD) be conducted regarding the relevant parties, and may arrange for support from external consultants if deemed necessary. Based on the assessment results, the relevant business and operations unit informs senior management of the identified compliance risks, their potential impact on the Company, and recommendations regarding whether to proceed with the transaction or terminate it. Senior management reviews the assessment and recommendations and decides whether to proceed with the transaction, suspend it, or continue it under specific conditions; if deemed necessary, approval from the Board of Directors is sought. Decisions made and processes carried out may be reported and evaluated within the scope of internal audit as deemed necessary. Relevant units or employees consult the Legal and Compliance Department if they have any doubts regarding the actions to be taken.

---

<sup>6</sup> Business and operational units must exercise special caution regarding business relationships and transactions with natural and legal persons, unincorporated entities, and citizens of high-risk countries; they are required to gather information to the extent possible regarding the purpose and nature of transactions that lack an apparent reasonable legal or economic purpose, and to document such information.

The Company ensures that contracts to be signed with Business Partners include compliance obligations with this Policy to the extent appropriate and reserves the right to terminate the contract or apply other contractual sanctions in the event of a violation of this Policy.

## 4.2. Suspicious Transactions

Company employees are expected to remain vigilant at all times regarding signs of AML-CFT risks. If, during the course of any transaction, there is any suspicion that the assets involved were obtained through illegal means or are being used for illegal purposes—including, but not limited to, the financing of terrorism—or are related to or connected with such activities, the transaction must be immediately reported to the Legal and Compliance Department via the Suspicious Transaction Forms at<sup>7</sup>.

The following transactions and activities may be considered examples of suspicious transactions:

- Providing incomplete, incorrect, contradictory, or suspicious information, or exhibiting hesitation, reluctance, or creating difficulties regarding compliance with reporting and/or record-keeping requirements,
- Requests for payments to be made specifically in cash or cash equivalents, or to be executed into different bank accounts on behalf of third parties,
- Transactions and individuals associated with countries designated by the FATF as high-risk<sup>8 9</sup>,
- Payments made in currencies other than those specified in the contracts, the use of cryptocurrencies in transactions, or requests for such payments,
- Making payments to third parties not named in the relevant contracts, receiving payments from such third parties, or using currency exchange offices as intermediaries in transactions,
- Payments made to “shell bank” accounts or to individuals or entities residing in countries known as “tax havens,” or fund transfers to or from foreign countries unrelated to the transaction,
- Payments made to or from entities where it is not possible to determine the ownership structure or identify the Ultimate Beneficial Owner (UBO),
- Transactions linked to individuals listed on money laundering watchlists, as identified through screening tools,
- Payments made in small, incremental amounts through multiple different financial institutions.

---

<sup>7</sup> Suspicious Transaction Reports must be prepared by the Office of the General Counsel and Compliance and shared with business and operational units

<sup>8</sup> <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions.html>

<sup>9</sup> As of the effective date of this Policy, North Korea, Iran, and Myanmar are listed on the FATF’s High-Risk Countries list. Stricter measures may be implemented and the list of high-risk countries may be expanded, subject to the opinion of the Legal and Compliance Advisory Office.

It is crucial that all employees remain vigilant in this regard and act decisively and in accordance with established procedures upon identifying a suspicious transaction; in case of any doubt, all employees may consult the Legal and Compliance Department.

### **4.3. Training**

Within the Company, under the coordination of the Legal and Compliance Department, training and awareness-raising activities are conducted to enhance awareness regarding the prevention of money laundering, the financing of terrorism, and the financing of weapons of mass destruction, and to foster a shared culture of compliance in this area. These activities are planned and implemented in accordance with applicable national and international legislation, this Policy, and relevant internal company regulations. Training activities aim to ensure that employees can identify compliance risks they may encounter within the scope of their duties and responsibilities, detect suspicious situations, and take necessary actions. Activities conducted within this scope may be monitored and reported as deemed necessary.

## **5. AUTHORITY AND RESPONSIBILITIES**

All employees and managers of the Company are responsible for complying with this Policy and for implementing and supporting the Company's relevant procedures and controls in accordance with the requirements of this Policy. To the extent applicable to the relevant party and transaction, the Company expects all Business Partners to act in compliance with this Policy and takes the necessary steps to ensure this.

In the event of a conflict between this Policy and local laws applicable in the countries where the Company operates, the more restrictive of the two—whether the Policy or the law—shall prevail, provided that such application does not conflict with local laws.

If you become aware of any action that you believe violates this Policy, applicable laws, or the Company's Code of Ethical Conduct, you may consult with your supervisor or report the matter to the Legal and Compliance Department. Alternatively, you may submit a written report through the email address [etik@ozaltin.com.tr](mailto:etik@ozaltin.com.tr), which is accessible to the Legal and Compliance Counsel and the Director of Audit and Organization, or submit an anonymous report through the Ethics Line Application Form available on the Company's website.

Company employees may consult the Legal and Compliance Department, which is responsible for compliance, regarding any questions about this Policy and its implementation. A violation of this Policy by an employee may result in various disciplinary actions, including termination, under the Labor Code, other relevant legislation, and the Company's internal policies and regulations. If any third party expected to comply with this Policy acts in violation of it, the relevant contracts may be terminated.

**6. EFFECTIVE DATE**

This Policy entered into effect pursuant to the Board of Directors' Resolution dated April 28, 2026, and the Legal and Compliance Department is responsible for updating the Policy.

<b>Revision</b>	<b>Date</b>	<b>Description</b>
1	April 28, 2026	Review
2	May 14, 2026	The Ethics Line Application Form has been added to the whistleblowing reporting channels.