Ermenegildo Zegna Group

ANTI-MONEY LAUNDERING AND SANCTIONS POLICY

(as adopted on April 5, 2023)

INDEX

1. INTRODUCTION & POLICY PURPOSE

Ermenegildo Zegna N.V. is committed to ensuring that it and all of its subsidiaries and associates[1] (collectively, "the Group") prevent its business from being used to facilitate financial crimes, including money laundering, terrorist financing, and violations of any applicable sanctions laws and regulations in each jurisdiction in which the Group operates.

The Group has voluntarily adopted this risk-based Anti-Money Laundering ("AML") and Sanctions Policy (the "Policy") to protect itself, its directors, and employees, to the extent reasonably possible, from being used to facilitate money laundering, terrorist financing, violations of economic sanctions, and other financial crime.

The Group bases all actions, operations, dealings and transactions undertaken in the course of its business activities on the ethical principles and rules of conduct set out in this Policy and the Group's Code of Ethics. Additionally, the Policy should be read together with other relevant policies, including but not limited to the Group's Code of Ethics and Misconduct Reporting Policy.

2. SCOPE OF APPLICATION

This Policy is binding on all Group directors and officers, those who, within the Group companies (including joint ventures), carry out functions of representation, administration or management or who exercise management and control, as well as on all Group employees and representatives (e.g., freelance consultants, suppliers, agents, distributors, representatives, brokers, etc.) (hereafter "Persons subject to this Policy").

Persons subject to this Policy must, therefore, be aware of the provisions of this Policy and the employees of Group companies are called upon to play an active role in ensuring that it is complied with. For this purpose, the Group undertakes to ensure that this Policy is distributed as widely as possible and incorporated into employee training to raise awareness of its content.

All Persons subject to this Policy are responsible for reading and understanding the Policy. Any activities by Persons subject to this Policy that violate this Policy or any AML or relevant sanctions requirements are strictly prohibited. Any questions about the Policy or its application to a specific business area should be directed to Group Compliance & Risk Management Function (compliance@zegna.com).

[1] With respect to any subsidiary or associate that Ermenegildo Zegna N.V. does not, directly or indirectly, control, it will use its reasonable best efforts to influence such non-controlled entities to adhere to this Policy.

3. PERSONS RESPONSIBLE FOR APPROVAL AND IMPLEMENTATION OF THIS POLICY

The Group Chief Compliance Officer ("GCCO") will monitor the Group's compliance with the Policy.

The Policy focuses primarily on compliance with AML and sanctions laws and regulations imposed by the United States (the "U.S.") and the European Union (the "EU"). However, the Group must remain equally attentive to compliance with all applicable laws and regulations in each jurisdiction in which the Group operates. The GCCO must develop local monitoring mechanisms, generally in consultation with local legal departments, with internal controls to ensure compliance with any additional local anti-money laundering or requirements with respect to any territory in which the local operation does business.

To ensure that changes to the Group's business are accurately reflected in the Policy, the Group will regularly review and update the Policy in response to changing risks. Based on the evolving risk profile of the Group and its operations (i.e., products, services, business lines, customers, and geographic locations), the Group will periodically develop and conduct appropriate risk assessments to identify vulnerabilities of the Group to potential violations of the relevant statutes, guidelines and standards, including with respect to abuse by criminals and other bad actors. Such assessments will also be used for providing updates, as necessary, to the Group's overall AML and sanctions risk profiles. The GCCO will also work with business areas to identify areas of particular risk and establish appropriate procedures and mitigating internal controls and respond to any questions about the Policy. As appropriate, the risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the Group during the routine course of business. As a part of the risk assessment, the Group shall consider, among other things, how resources should be deployed to address higher risk areas and whether any changes should be made to this Policy. The GCCO will be responsible for conducting the risk assessments and will review and re-evaluate the Group's risk assessments as necessary, but not less than once every three years.

The GCCO will undertake periodic AML and sanctions compliance reviews or audits to test and monitor the ongoing effectiveness of the Policy and its application to the businesses of the Group.

The GCCO will liaise with local law enforcement and regulatory authorities with regard to any money laundering or sanctions issues.

The GCCO will ensure the proper retention of AML- and sanctions-related records, in accordance with the Group's record retention policy.

The GCCO will provide or arrange for the provision of training to employees at least annually. Certain employees will be identified and trained by the GCCO to perform customer due diligence ("CDD") and sanctions compliance screening procedures for customers and counterparties (collectively, "customers") and any other third parties, such as agents, consultants, distributors, licensees, re-sellers, suppliers, and other third parties who operate in any capacity on behalf of the Group (collectively, "third parties") in compliance with the Policy. The GCCO will incorporate AML and sanctions compliance into the job descriptions and performance evaluations of employees, as appropriate.

The GCCO may periodically amend and recirculate the Policy with the consent of the Board of Directors. The GCCO will periodically report to the Audit Committee on the status of the processes and procedures in place to avoid sanctions and money laundering-related violations.

4. LEGAL FRAMEWORK FOR MONEY LAUNDERING

The Group seeks to comply with all applicable anti-money laundering laws, regulations, and conventions, including: the United States Money Laundering Control Act; the laws of EU member states implementing EU Directive 2015/849 (as amended) on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing (the "EU AML Directives")[2]; in the United Kingdom, the Proceeds of Crime Act 2002 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended), which essentially incorporate the EU AML Directive into UK law; the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force (the FATF Recommendations); and other similar anti-money laundering laws and authorities in other jurisdictions in which the Group operates.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the origins of proceeds derived from criminal activity by creating the appearance that the proceeds are derived from a legitimate source. These proceeds may include profits from drug trafficking, embezzlement, corruption, fraud, or other federal, state, or foreign criminal offenses. Money laundering is not limited to cash transactions – it may include non-cash transactions (such as wire transfers or credit card purchases), foreign exchange transactions, and real estate transactions. Money laundering usually consists of three fundamental components: placement, layering and integration.

[2] Each EU member state has its own national legislation that incorporates the provisions of the EU AML Directive into national law. EU AML laws are enforced by the relevant national authorities and not by any central EU authority.

Placement. Cash first enters the financial system at the placement stage, where cash from criminal proceeds is deposited into a bank or other depository or financial institution, or converted into negotiable monetary instruments, such as money orders or traveler's checks. To disguise criminal activity, cash sometimes is also routed through a "front" operation business, such as, for example, a check cashing service.

Layering. This stage refers to the creation of complex or multiple layers of transactions that are intended to break the audit trail from the illegal source by further separating the funds from its criminal origin. The funds can be transferred or moved into other accounts, financial institutions, shell companies, or disguised as the proceeds of legitimate business.

Layering sometimes is accomplished by transferring funds to countries that have strict bank secrecy laws, such as, for example, the Cayman Islands, the Bahamas and Panama. These secrecy laws and the high daily volume of wire transfers can make it difficult for law enforcement agencies to trace these transactions. Once deposited in a foreign bank, the funds can be moved through accounts of "shell" corporations that exist solely for money laundering purposes.

Integration. At this stage, funds are moved into the financial system and are made to appear to have been derived from legitimate sources. The money is therefore re-introduced into the economy and may be used to purchase legitimate assets or to fund other criminal activities. Examples include making loan repayments, creating a new business with the laundered money, and mixing laundered money with income from other legitimate income or assets. Other examples include trade-based money laundering schemes, which involve the deposit of criminal proceeds into a U.S. or EU bank account(s) that are then transferred to a business to purchase goods, which are then shipped to foreign countries for sale, with the sale proceeds being transferred to the criminal organization, making the funds obtained illicitly in the U.S. or EU look as though they are legitimate.

5. LEGAL FRAMEWORK FOR SANCTIONS

Sanctions are typically imposed by a government or an international organization to achieve a variety of foreign policy or national security objectives and generally are restrictions on the ability of an entity or individual to engage in certain commercial activities and financial dealings with targeted entities or individuals. Sanctions measures can vary from the comprehensive – prohibiting trade with a target country and freezing the assets of a government, the corporate entities and residents of that country – to targeted asset freezes on specified entities or individuals. The Group will conduct its activities in compliance with the sanctions requirements of the U.S., EU, and any other jurisdiction that the Group Chief Compliance Officer determines.

Certain entities and individuals targeted by Sanctions are identified on lists issued by the U.S., EU, United Nations and other governments or international organizations, which are published on websites and are publicly available ("Sanctions Lists"). Sanctions also target certain entities and individuals not included on these Sanctions Lists, including entities owned or controlled by entities or individuals on such lists.

Failure to comply with sanctions can lead to severe civil and criminal penalties, both for our business and individual employees, officers and directors, as well as significant reputational damage to the Group.

As a general rule, employees and representatives of the Group are not permitted to engage in any transactions or dealings with a party that is the target of applicable sanctions, such as the sanctions programs of the U.S. or the EU, or any jurisdiction that is the target of comprehensive sanctions. That does not, however, mean that all transactions involving a jurisdiction that is targeted by any sanctions will be off limits for the Group; some jurisdictions, such as the Russian Federation and the People's Republic of China, are targeted by more nuanced sanctions, and in those cases, certain transactions and dealings may be permissible, although caution is warranted. The relevant sanctions programs and targets, and how to identify them and the scope of coverage of the applicable sanctions, will be specified by the Group Chief Compliance Officer (collectively, the "Relevant Sanctions Programs"), and all questions regarding scope of coverage should be directed to the Group Chief Compliance Officer.

5.1 U.S. SANCTIONS

The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") administers and enforces U.S.-based economic and trade sanctions programs ("OFAC Sanctions Programs"), which are based on U.S. foreign policy and national security goals, as well as on United Nations and other international mandates. Additionally, OFAC publishes lists of individuals, groups and entities, such as terrorists and narcotics traffickers, which are the target of the OFAC Sanctions Programs. These include: the Specially Designated Nationals ("SDNs") and Blocked Persons List (the "SDN List").[3]

U.S. sanctions apply to:

- U.S. companies and their overseas branches (and, for certain sanctions, non-US subsidiaries of U.S. companies) in relation to anything they do anywhere in the world;
- U.S. citizens and permanent resident aliens (i.e. "green card" holders) in relation to anything they do anywhere in the world; and

[3]The U.S. Specially Designated Nationals and Blocked Persons List is available here: https://home.treasury.gov/policy issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

- Certain non-U.S. companies and non-U.S. nationals in relation to anything they do in the U.S. and any business conducted wholly or partly in the United States

U.S. sanctions can also be applied to transactions that touch or concern the United States, including those that take advantage of the U.S. financial system (e.g. dollar-denominated transactions) and those that involve U.S. companies and individuals or U.S.-origin items.

The United States has also implemented so-called "secondary sanctions" that provide for sanctions against companies and individuals who engage in specific kinds of transactions and dealings, generally targeting specified activities in sanctioned countries, such as Iran, even if the transaction or dealing does not otherwise have a U.S. jurisdictional nexus. These sanctions provide for the imposition of a range of measures designed to exclude or restrict the non-U.S. Person who engages in the conduct from U.S. economic activity.

5.2 EU SANCTIONS

The Council of the European Union takes decisions on the adoption of EU sanctions. The European Commission gives effect to these decisions into EU law through proposals for regulations, which are in turn adopted by the Council. There is, however, no central EU enforcement body, and enforcement of EU sanctions is a matter for individual Member States.

EU sanctions comprise a range of financial and trade measures. The main financial sanctions involve the designation of individuals or legal entities, resulting in their assets being frozen and a prohibition on funds or economic resources being made available to them. The EU maintains a consolidated list of individuals and legal entities subject to financial sanctions[4] Legal entities that are majority-owned or controlled by a person or entity included in the EU consolidated list are treated as if they were also included in the list. EU trade restrictions differ from country to country, but can extend to prohibitions on the import or export of a wide range of goods and technology, including luxury goods.

EU Sanctions apply to:

- EU companies and EU nationals in relation to activities anywhere in the world – even if an EU national is employed by a non-EU company; and
- Non-EU companies and non-EU nationals in relation to activities in the EU and any business they conduct wholly or partly in the EU.

The EU does not impose secondary sanctions.

[4] The EU's consolidated list is available here: https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en

6. AML AND SANCTIONS COMPLIANCE PROGRAM

The Group has voluntarily adopted this Policy to combat money laundering, terrorist financing, violations of economic sanctions, and other financial crime (the "Program"). The elements of the Program are discussed in the sections below:

(1) Employee Awareness and Training

All employees are responsible for reading and having access to the Policy. All employees will receive compulsory Policy training upon joining the Group [and then refresher training at least annually. In addition, the Group Chief Compliance Officer (GCCO) and all other employees who are identified as responsible for administering CDD questions or otherwise engaging in CDD functions will receive training on the appropriate processes and the use of tools that will be necessary or useful in performing their duties. Dates and names of those in attendance at the training will be recorded, with training materials and records kept for the required retention period.

The training will cover factors that employees who handle or supervise the handling of customers, transactions and/or funds that may involve suspicious activity should be aware of. The training will also cover, at a minimum, the following:

- The employees' responsibilities under the Policy, including the responsibility for obtaining sufficient CDD, and for identifying and escalating suspicious activity to the GCCO.
- Red flags and signs of money laundering, terrorist financing, and other financial crimes that arise during the course of the employee's duties.
- The identity and responsibilities of the GCCO.
- The potential consequences for employee non-compliance with applicable OFAC laws and regulations, including disciplinary action by the Group, as well as civil and criminal penalties.
- The Group's record retention policy in relation to the Policy.

The Group, in conjunction with the GCCO, will review its businesses to see if certain employees, depending on the business area in which they work, may need to receive further or more specific training, which will be recorded and retained in the same manner as the Group-wide Policy training. Additionally, the Group's senior management will receive high-level training and awareness that will be designed to foster the Group's top-level commitment to complying with the Policy.

(2) Audits

The GCCO will undertake periodic AML and sanctions compliance reviews or audits to test and monitor the ongoing effectiveness of the Program and the Program's application to the Group. To the extent deemed useful and appropriate, the GCCO will arrange for external audits performed by a third-party provider for purposes of gap analysis and testing the appropriateness of the Group's controls in light of the risk profile of the Group. To the extent that such external audits are undertaken, the scope will be defined by the GCCO, working with the external auditor.

(3) Customer Due Diligence

The CDD process is an important process to held enable the Group to know more about the parties with which it is transacting and dealing and is an important part of the tools that the Group uses to detect, prevent, and where appropriate, report money laundering, terrorist financing, and other illicit activity. The CDD process also assists the Group to comply with AML laws and sanctions applicable to the Group.

As a general rule, the Group applies a risk-based approach to AML and sanctions compliance. Only those counterparties and transactions which present identified risk factors are further examined to determine whether they implicate applicable AML laws or sanctions. If there is any doubt, consult the Compliance & Risk Management Function, available at compliance@zegna.com .

Although the process is referred to as the "customer due diligence" process, the scope of the CDD process is not limited to retail customers. The Group will perform CDD on customers, but also on transaction parties, such as suppliers, distributors, wholesalers, marketing representatives and other counterparties, based on appropriate risk assessments. The party responsible for identification and independent verification of the identity of such parties, and, where appropriate, their owners, controlling parties and potential nexus to any sanctioned jurisdiction or person will vary depending on the situation. Counterparties at the Group level typically will be reviewed by or at the direction of the GCCO. Local relationships may be reviewed by local Group personnel, although the GCCO may provide important guidance to local Group personnel.

Based on the Group's risk assessments, the GCCO will generally determine appropriate screening, customer declarations, and other measures appropriate to the risk profile of the Group that can be used to perform CDD. The Group generally will conduct enhanced due diligence on counterparties whom it determines to be high-risk, including Politically Exposed Persons ("PEPs").[5] For certain low-risk and standard-risk customers, or in purely retail store settings for

[5] PEPs are defined as natural persons who are or have been entrusted with prominent public functions, which would include, for example, senior politicians, senior government, judicial or

customers who are not "regulars", it may be appropriate for the Group to conduct no, or only limited, due diligence. For example, in a retail store setting, it may be difficult to obtain detailed CDD information in the ordinary course of transactional expectations. Retail store personnel should nevertheless be sensitive to "red flags" exhibited by retail store customers and be prepared to report examples to the GCCO for further action,

Example 1: A retail customer who is a PEP regularly purchases a quantity of items at a single retail location that appears significantly disproportionate to his or her expected income. The customer may present an anti-money laundering risk, and further due diligence should be considered.

Example 2: A retail customer purchases a number of items in a short time in a series of transactions through the Company's principal website, and provides a credit card that does not match the retail customer's name, or the Company experiences a high percentage of card rejections. The customer may present an anti-money laundering risk, and further due diligence should be considered.

Example 3: The Group is solicited to sell products to a wholesaler that has distributors in a sanctioned jurisdiction. The wholesaler presents a sanctions risk. Both the wholesaler and its distributors should be screened.

Example 4: The Group is solicited to regularly purchase large quantities of textiles from a company with a line of business apparently incongruent with such purchases and that presents suspicious identification that cannot be verified, such as a disconnected telephone number. The textile supplier presents an anti-money laundering risk and should be screened.

Identification and verification requirements will vary between the Group's business lines, and responsibility for the completion of the CDD process may fall on employees, third parties who operate and manage the Group's business lines, or contractors the Group hires to complete the CDD process.

In circumstances where a business transaction involves a potential AML violation or nexus to a sanctioned party or country, the transaction or any attempted transaction must be reported to the GCCO, who will ensure to keep of a record of relevant details and, as appropriate, in consultation with external counsel, determine if the activity should be reported to the relevant authorities or if the transaction should be blocked or rejected in compliance with Relevant Sanctions Programs.

---

military officials or senior executives of state-owned corporations, as well as immediate family members, or persons known to be close associates, of such persons.

As part of the CDD process, before entering into a relationship with any customers or other third parties such as suppliers, licensors, licensees, resellers, distributors, or other service providers, the Group will consider whether it needs to include relevant contract provisions stating that the third party is compliant with applicable AML laws and Relevant Sanctions Programs.

Additionally, the Group will periodically screen its customer base for any nexus to a Relevant Sanctions Program. Such screening will be based on the evolving risk profile of the Group and will occur as appropriate and annually on the Group's customer base.

(4) Provision of CDD/UBO Information Regarding the Group

In certain situations, the Group may be asked to provide CDD or ultimate beneficial owner ("UBO") information about the Group. For example, financial institutions regularly solicit CDD and UBO information as part of those institutions' AML and sanctions compliance programs. In order to ensure consistency and appropriate responses to such questions, any request received by a member or employee of the Group should be referred the request to the GCCO, who will ensure that information is provided for the Group as necessary and appropriate for the relationship in question.

7. RETENTION OF RECORDS

If a customer comes under investigation by the authorities for activity related to AML or sanctions compliance, the Group must be able to provide an audit trail of the processes undertaken pursuant to the Policy. The employees of the Group's Compliance & Risk Management Function, including the GCCO, responsible for AML- and sanctions-related compliance, must retain all customer AML and sanctions due diligence records, including records on the customer's identity and transactions, and Group reports on such customers and transactions, in accordance with the Group's record retention policies related to the Policy. These include:

- Records in relation to the identity of the customer obtained in the CDD process, including a copy of the evidence of identity obtained or a record of where a copy of the evidence of identity can be obtained;
- Records of action taken or reports made with respect to the internal and external reporting of suspicious activities;
- Records relating to the Group's screening processes for sanctions compliance with respect to its customers;
- Records of the dates of and topics covered by Policy training;
- Copies of any reports generated by the Group Chief Compliance Officer with respect to any exemptions from or any waivers of any of the Policy requirements; and
- Other books and records as required by the Group's record retention policies.

Complete and accurate records must be retained by employees of the Group's Compliance & Risk Management Function responsible for AML- and sanctions-related compliance, including the GCCO, and kept retrievable during the relationship with the customer and until at least five years from the date when the relationship with the customer ends.

All records concerning hits or matches to a relevant Sanctions List, as well as records concerning blocked property or rejected transactions, will be maintained for a period of five years. If a transaction is blocked, the records related to such blocked property will be maintained for a period of five years after the date when such property is unblocked.

Records that relate to current investigations, or activities that have been disclosed to the authorities, should be retained pending agreement by the authorities that records may be destroyed.

8. OBLIGATIONS OF PERSONS SUBJECT TO THIS POLICY

Persons subject to this Policy, regardless of their location or position, and all those acting on their behalf, have the following obligations:

- Adhere to all applicable AML and sanctions laws and regulations, in all jurisdictions in which the Group operates.
- Familiarize themselves with this Policy, distribute and explain the Policy to subordinates and third parties acting on the Group's behalf, and act at all times in accordance with this Policy.
- Raise questions to the Group's Compliance & Risk Management Function regarding any uncertainty as to whether a transaction or activity would violate an applicable AML or sanctions law or regulation.
- Accurately record all transactions, particularly all required details and approvals of transactions, and maintain complete and accurate books and records.
- Conduct appropriate customer due diligence and sanctions screening before engaging with any new business partner or retaining any third party to act on behalf of the Group.
- Manage and monitor business activities conducted on behalf of the Group by third parties.
- Be alert to indications or evidence of suspicious transaction activity or structuring in connection with the Group's business.
- Participate in required compliance training related to this Policy.
- Promptly report violations or suspected violations of this Policy or any AML or sanctions law or regulation, as required by Section 4 of Misconduct Reporting Policy.

9. RED FLAGS

Be alert to the following "Red Flags" and seek the assistance of the Compliance & Risk Management Function in resolving any doubts before proceeding with the transactions or activity to which the concerns relate.

Red Flags

- A customer provides insufficient or suspicious information.
- A customer uses suspicious identification documents that cannot be readily verified.
- A business is reluctant to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- The customer's background differs from that which would be expected on the basis of his or her business activities.
- Payments for goods or services are made by checks, money orders, or bank drafts not drawn from the account of the entity that made the purchase.
- Use of corporate vehicles (i.e. legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions.
- Use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- A customer or group tries to persuade an employee not to maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- Goods or services purchased by the business do not match the customer's stated line of business.

10. REPORTING VIOLATIONS

It is the responsibility of all individuals working with or for the Zegna Group to report any potential violations of this Policy or any anti-money laundering or sanctions laws. If you suspect that a violation of this Policy or any anti-money laundering or sanctions laws has occurred, you must immediately report that suspicion through as required by Section 4 of the Misconduct Reporting Policy.

No employee will suffer demotion, penalty or any other adverse consequence for making a report in good faith or otherwise following the Policy, even if such actions results in a loss of business or other adverse consequence to the business.