Sanctions and Compliance Policy

Group policy

xstreco

Contents

Approved by	The Board of Directors of Xstreco AG
Issued by	Executive management
Issued on	01.09.2026
Version	2.1

1 Introduction

1.1 Purpose and Scope

1.1.1 Purpose of the Policy

This policy sets out the controls required so that the Group complies with the sanctions, export controls and restrictive measures that apply to it, and manages the exposure arising from those that apply to its counterparties.

1.1.2 Scope and Applicability

This policy applies to all employees, directors, officers, and contractors under Xstreco's direct supervision, working for any Xstreco office or industrial asset directly or indirectly controlled or operated by Xstreco worldwide. Where the Group holds an interest in a joint venture that it does not control or operate, it uses its influence to encourage conduct consistent with this policy.

2 Policy Statement

2.1 Group's Stance on Sanctions and Compliance

The Group must comply with the sanctions, export controls and restrictive measures that apply to it. Transactions designed to evade sanctions or export controls, or to facilitate a breach of them, are prohibited. Business with a party subject to blocking sanctions, and business with an embargoed territory, are prohibited. Where a party is subject to sectoral sanctions, any dealing falling within the restricted sector or activity is prohibited, and any other dealing with that party must be cleared by the compliance function before the Group proceeds. The export, transit, brokerage or re-export of goods, software or technology that is subject to export controls must be cleared as section 3.1 requires.

2.2 Legal Implications

Swiss sanctions are imposed under the Embargo Act (SR 946.231) and the ordinances made under it, which give effect to measures decided by the United Nations, the OSCE, and Switzerland's most important trading partners; the export, transit and brokerage of dual-use goods, specific military goods and strategic goods are governed by the Goods Control Act (SR 946.202). SECO administers both. In Peru, there is no autonomous sanctions regime; United Nations Security Council measures are given effect through the anti-money laundering framework administered by the Financial Intelligence Unit. The Group is not established in the European Union or the United States, so the measures of those jurisdictions do not apply to it by reason of incorporation; they may nonetheless bind it directly, as European Union restrictive measures do in respect of business done wholly or partly within the Union, and a person subject to this policy who is a national of a Member State of the European Union or a United States person is directly bound by the measures of that jurisdiction. The Group is also directly subject to United States export controls in respect of goods, software and technology of United States origin, including their re-export from one foreign country to another, and it may be exposed to United States measures through secondary sanctions and through settlement and financing arrangements; and any Group entity that came to be incorporated or constituted in the European Union or the United States would be directly subject to the measures of that jurisdiction. The policy takes account of the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, which are recommendations to enterprises and not binding law. Non-compliance with this policy, and the conduct it prohibits, may result in reputational damage, legal penalties, and internal disciplinary action.

3 Key Principles and Guidelines

3.1 Specific Principles or Guidelines

This policy requires the following principles to be applied:

(a) Counterparty and Transaction Screening: Counterparties are screened on a risk basis against the SECO, UN and EU restricted party lists, against the lists maintained by the United States Office of Foreign Assets Control (OFAC) where relevant to the dealing, and against the lists of any other jurisdiction relevant to the dealing, and transactions are reviewed on the same basis for sanctions exposure. Where the Group's activities come to involve the carriage of goods, the screening arrangements extend to vessels and shipments.

(a) Risk-Based Due Diligence: Enhanced sanctions due diligence must be conducted for jurisdictions, sectors and counterparties that are subject to measures administered by SECO, that are, or are connected with, a jurisdiction identified as high risk by the Financial Action Task Force, or that the Group's own risk assessment identifies as high risk, including establishing beneficial ownership.

(b) Export Control Classification and Clearance: Goods, software and technology that the Group exports, moves in transit, brokers or re-exports must be assessed on a risk basis to establish whether they are subject to export controls, and an item that is subject to them must be cleared by the compliance function, and licensed where a licence is required, before the activity proceeds.

(c) Payment Controls: Payment processes must be designed to identify, and to prevent, payments involving a sanctioned party or jurisdiction.

(d) Escalation and Approval: A sanctions concern identified in a dealing is referred to the compliance function for assessment before that dealing proceeds. External legal advice is taken where the position is uncertain.

(e) Record Keeping and Audit Trails: Screening, due diligence and the reasons for decisions must be documented and retained for the period the law applicable to them requires and, subject to that period, in accordance with the retention arrangements required by the Information Governance and Security Policy.

(f) Transparency with Banks and Authorities: Information lawfully required by a financial institution or an authority in connection with sanctions compliance must be provided promptly and accurately.

3.2 Examples and Applications

(a) Screening a Sanctioned Entity: Screening of a potential supplier during onboarding returns a match that the compliance function confirms. The relationship must not be entered into.

(b) Rejecting a Restricted Transaction: A bank blocks a payment on a sanctions match. The compliance function assesses the match and determines whether the transaction is prohibited.

(c) Responding to a Sanctions Alert: Screening returns a possible match against a restricted party. The dealing must be halted and the match escalated to the compliance function for resolution before the Group proceeds.

(d) Escalating a High-Risk Jurisdiction: A proposed transaction connected with a high-risk jurisdiction must be referred to the compliance function and cleared before the Group proceeds, and external legal advice taken where the position is uncertain.

4 Roles and Responsibilities

4.1 The Board

Oversight of this policy rests with the board. The board approves this policy and each revision of it.

4.2 Executive Management

Executive management issues this policy, provides the means required to apply it, and is accountable to the board for its application. Where this policy requires a matter to be escalated, it is escalated to executive management.

4.3 Responsibility for This Policy

Responsibility for the day-to-day application of this policy is assigned within the Group. This policy requires that the assignment be recorded in the Schedule of Policy Assignments, an internal document, be kept current, and be made known to those subject to this policy. Where this policy refers to the compliance function, it means the person or persons holding that assignment at the relevant time, whether or not a separate department exists.

4.4 Those Who Direct the Work of Others

Anyone who directs the work of others is responsible for applying this policy in the work they direct, for making those they direct aware of it, and for passing on a concern raised with them.

4.5 Everyone Subject to This Policy

Everyone subject to this policy must comply with it, must raise a concern where they believe it has been or may be breached, and must co-operate with any enquiry into such a concern.

4.6 Counterparties

Counterparties must meet the standards in this policy where their contract with the Group so provides, and may raise a concern through the channels in section 5.1.

4.7 Those Responsible for Counterparties and Payments

Those responsible for engaging a counterparty, or for making or receiving a payment, are responsible for the screening this policy requires before the Group is committed, and for referring any possible exposure to the compliance function before proceeding. The means of screening are proportionate to the counterparties and payments actually involved.

5 Reporting and Monitoring

5.1 Reporting Mechanisms

5.1.1 Internal Reporting

A concern under this policy may be raised with a line manager, with any member of executive management, or with the compliance function. A concern may also be raised through the web reporting form at xstreco.com/report, by writing to compliance@xstreco.com or codeofconduct@xstreco.com, both of which reach the compliance function, or by telephone on +41 41 562 32 90, asking for the compliance function. Retaliation against a person who raises a concern in good faith is prohibited.

5.1.2 External Reporting

A person who is not employed by the Group may raise a concern through the web reporting form at xstreco.com/report, by writing to compliance@xstreco.com or codeofconduct@xstreco.com, by telephone on +41 41 562 32 90, or by post, marked 'Confidential - Compliance', to the address at the end of this document. A concern may be raised in English or in Spanish. A name and contact details are not required, and a concern raised without them is assessed in the same way. The Group's website provider records basic technical data with every submission, so a report made through the form is not technically anonymous, and a call is not anonymous; a report sent by post can be.

5.2 Monitoring Procedures

This policy requires that its application be kept under review, and that a record sufficient to show how it has been applied be kept. In particular, this policy requires:

(a) that compliance with this policy be reviewed on the cycle stated in section 8;

(b) that concerns raised under this policy, and the way in which each was resolved, be recorded;

(c) that the risk this policy addresses be reassessed whenever the Group's activities change materially;

(d) that matters which are unresolved, which recur, or which are systemic be escalated to executive management and, where the law requires it or it is otherwise appropriate, to the competent authorities;

(e) that those subject to this policy be able to demonstrate, from the records kept, that its requirements were met.

The means used to meet these requirements are proportionate to the size of the Group and to the scale and nature of its activities at the time, and are extended as those change.

6 Training and Awareness

6.1 Awareness on Appointment

This policy requires that everyone subject to it be made aware of it on appointment and be given the instruction needed to apply it in their role. The form and the depth of that instruction are proportionate to the role.

6.2 Continuing Awareness

This policy requires that awareness of it be refreshed on the cycle stated in section 8, and whenever the policy is revised or an event makes it necessary, and that those in roles carrying greater exposure to the risk this policy addresses receive instruction appropriate to that exposure.

7 Compliance and Consequences

7.1 Reporting Non-Compliance

Everyone subject to this policy must report suspected violations, as must counterparties where their contract with the Group so provides. The identity of the person making a report is treated as confidential and is not disclosed except where disclosure is required by law or is necessary for the enquiry, and then only to the extent necessary. Retaliation against a person who reports in good faith is prohibited.

7.2 Consequences of Non-Compliance

Violations may result in disciplinary action, including termination of employment or contract, and may trigger legal proceedings.

8 Review and Revision

8.1 Review Frequency

8.1.1 Review Cycle

This policy is reviewed at least once in every two calendar years.

8.1.2 Event-Triggered Review

A review is carried out, whether or not one is due under the cycle, whenever a change in the law, a material change in the Group's activities, or an event arising under this policy makes one necessary.

8.1.3 Conduct and Outcome of the Review

The review is carried out by the holder of the responsibility described in section 4.3. Its outcome is submitted to the board, and any revision resulting from it is approved by the board before issue.

8.2 Revision History

8.2.1 Version 2.1 - 01.09.2026

Approved by the board and issued by executive management following a scheduled review of the suite. The amendments are editorial and clarifying; the policy positions stated in version 2.0 are unchanged.

8.2.2 Version 2.0 - 01.01.2026

Approved by the board and issued by executive management, replacing the first issue.

8.2.3 Version 1.0 - 02.06.2025

First issue.

8.2.4 Superseded Versions

Superseded versions are retained. Each revision is communicated to those subject to this policy.

9 Appendices

9.1 Glossary of Terms

(a) Sanctions: Legal measures that restrict trade, financial transactions, or other activities with specific entities or jurisdictions.

(b) Embargo: A government-imposed restriction on trade with a specific country or region.

(c) Restricted Party: An individual or entity subject to sanctions or other restrictive measures.

(d) Sanctions Due Diligence: The process of assessing the sanctions exposure and risk profile of business partners.

(e) Beneficial Owner: The natural person who ultimately owns or controls an account, entity or transaction.

(f) Blocking Sanctions: Measures that freeze assets and prohibit transactions with designated parties.

(g) Sectoral Sanctions: Restrictions on specific sectors or activities, such as finance or energy, without full asset freezes.

9.2 Related Legislation

9.2.1 Local Legislation

In Switzerland, the Embargo Act (SR 946.231) and the Goods Control Act (SR 946.202), both administered by SECO. In Peru, there is no autonomous sanctions regime; United Nations Security Council measures are given effect through the anti-money laundering framework administered by the Financial Intelligence Unit, including the freezing of funds under Ley N.° 27693, as amended.

9.2.2 International Standards and Frameworks

(a) UN Sanctions Regime: Binding on States; framework for implementing sanctions to maintain or restore international peace and security.

(b) EU restrictive measures: Binding law within their scope. They apply within the territory of the Union, including its airspace; on board aircraft and vessels under the jurisdiction of a Member State; to nationals of Member States wherever located; to legal persons incorporated or constituted under the law of a Member State wherever they do business; and to any legal person in respect of business done wholly or partly within the Union.

(c) United States sanctions and export controls: Binding law within their scope. They apply to United States citizens and permanent residents wherever located; to individuals and entities within the United States; to entities organised under the law of the United States or of a jurisdiction within it, and their foreign branches; under certain sanctions programmes, to foreign subsidiaries owned or controlled by United States persons; and, in respect of goods, software and technology of United States origin, including their re-export from one foreign country to another, to persons who are not United States persons. Secondary sanctions may attach consequences to conduct outside the United States.

(d) OECD Guidelines for Multinational Enterprises on Responsible Business Conduct: Recommendations to enterprises. Not binding law.

"Xstreco's policies set the standards that govern how the Group conducts its activities and how that conduct is assessed."

Xstreco AG
General-Guisan-Strasse 6
CH-6300 Zug
Switzerland

Email info@xstreco.com
Web xstreco.com