

TELUS

Sanctions Policy



Table of contents

i.	Introduction and purpose	3
ii.	Scope and application	4
iii.	Definitions	5
iv.	Responsibilities	6
v.	Compliance controls	7
vi.	Insulation of U.S., EU, UK persons	8
vii.	Record retention	9
viii.	Training and education	10
ix.	Guidance and reporting	11
x.	Policy review	12
	Appendix A: Red Flags of Potential Sanctions Evasion	13

i. Introduction and purpose

At TELUS, we take pride in being a global leader in ethical business practices. How we work is just as important as what we do. Our goal is to demonstrate the highest level of ethics and integrity in all of our dealings with customers, suppliers, governments, our team members and other stakeholders. This is a responsibility shared by everyone across our entire TELUS team and outlined in more detail in our [Code of Ethics and Conduct](#).

Complying with international sanctions regulations helps mitigate legal risks and potential fines. Compliance enhances a company's reputation and credibility, building trust with clients, partners, and stakeholders. It also safeguards against financial losses from asset freezes and operational disruptions that result from engaging with sanctioned entities. Moreover, a proactive compliance stance can provide a competitive edge, as it demonstrates a commitment to ethical practices and risk management.

The purpose of this Policy is to set out our approach to ensuring that we fully comply with all sanctions applicable to our business activities and that we appropriately manage associated risks.



ii. Scope and application of this policy

This Policy applies to all TELUS team members and Third Parties.

For TELUS team members: All TELUS team members must review and comply with this Policy in all jurisdictions where TELUS operates and are responsible for conducting appropriate screening and due diligence on counterparties before engaging in any transactions or entering into agreements. If a conflict exists between this Policy and local law, the Policy's standard must be followed, even if local law permits the conduct. If applicable laws require a higher standard of conduct, that higher standard must be followed. Any conflict between this Policy and Sanctions Laws must be resolved in favor of the more stringent standard.

For Third Parties: Third Parties must meet ethical standards consistent with industry standards and this Policy, comply with all applicable laws, including Sanctions Laws, and must not engage in any form of sanctions evasion. In the case of TELUS suppliers, they must also adhere to the TELUS Supplier Due Diligence Policy.

This Policy supplements other related TELUS policies, including the TELUS Anti-Bribery & Corruption Policy and the TELUS Supplier Due Diligence Policy. In the event of any inconsistency between this Policy and any other document (including any work instruction, standard operating procedure, or form), the terms of this Policy will prevail.

TELUS' Chief Data & Trust Officer is responsible for implementing this Policy with support from TELUS Legal, to assist the company and TELUS team members in complying with these requirements.



iii. Definitions

In this document:

“Policy” means this Sanctions Policy.

“Restricted Parties” means:

- a person or entity listed by OFAC as a Specially Designated National (“SDN”) or other OFAC sanctions target (e.g., a government or resident of an Embargoed Country or an entity owned 50% or more by an SDN);
- a person or entity listed by the U.S. Department of Commerce as a U.S. export restricted party;
- a person or entity designated under EU Sanctions Laws (including any person or entity included in the EU sanctions list, or any entity owned 50% or more, or otherwise controlled, by such a person);
- a person or entity designated under UK Sanctions Laws (including any person or entity included in the UK sanctions list, or any entity owned in excess of 50%, or otherwise controlled, directly or indirectly, by such a person); or
- a person or entity that is designated as a sanctions target under the laws of other jurisdictions in which the Company operates.

“Sanctions Laws” means all applicable laws, statutes, and regulations in place at the time of the relevant transaction and related to economic and trade sanctions imposed and administered by any governmental authority or international organization, including those administered by the Sanctions Bureau of Global Affairs Canada, the U.S. Department of the Treasury’s Office of Foreign Assets Controls (“OFAC”), the U.S. Department of State, the United Nations Security Council, the European Union (“EU”), and the United Kingdom’s Office of Financial Sanctions Implementation (“OFSI”).

“SDN List” means the list, published by OFAC, of individuals and companies owned or controlled by, or acting for or on behalf of, countries which are sanctioned by OFAC. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under OFAC programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs."

“TELUS” means TELUS Corporation or any of its subsidiaries.

“TELUS team members” or “team members” means the directors, officers and employees of TELUS.

"Third Parties" means all external entities and individuals acting on behalf of TELUS (including consultants, contractors, suppliers, and outsourced business associates).

“U.S. Persons” include all entities organized under U.S. law, all persons in the United States, and any U.S. citizens or U.S. green card holders globally.

iv. Responsibilities

Before engaging in any transactions or entering into agreements, team members must adhere to the controls and processes TELUS has in place to ensure compliance with Sanctions Laws. Team members should also look for indicators of sanctions evasion, such as those outlined in Appendix A. Where a team member is concerned that a transaction may violate Sanctions Laws or that certain actions may constitute evasion, they must place a hold on the transaction and immediately consult with their leader and TELUS Legal. The transaction or action must not resume without the written approval of TELUS Legal and the relevant business unit Vice President.



v. Compliance controls

To ensure compliance with Sanctions Laws, TELUS has a variety of controls and processes in place. These include:

- screening of, and due diligence on, its counterparties such as customers, vendors, suppliers and agents against restricted party lists (including those maintained by U.S., EU and UK authorities, such as the U.S. SDN List);
- prohibiting conduct designed or intended to evade or circumvent Sanctions Laws;
- maintenance of an “Embargoed Country” list;
- conducting ad hoc risk assessments as required in high-risk regions and monitoring any specific processes and controls;
- depending on the nature of the relationship, incorporating sanctions compliance obligations in commercial agreements with counterparties; and
- conducting periodic audits of compliance against this Policy.

The above list is not exhaustive and TELUS may adopt such other controls and processes it may deem necessary from time to time.

Should any contemplated transaction or customer relationship appear to involve a Restricted Party, directly or indirectly, the transaction or relationship may only proceed with the prior written approval of the Chief Legal and Governance Office of TELUS and the Vice-President with responsibility for the business unit in which the transaction arose.



vi. Insulation of U.S., EU, UK persons

TELUS is not a U.S. Person, all of its offices and TELUS team members in the United States and any TELUS team member globally who is a U.S. citizen or U.S. green card holder are U.S. Persons. In the absence of an applicable license, authorization or exception, U.S. Sanctions prohibit the involvement of U.S. Persons in transactions with OFAC sanctions targets. In the case of certain U.S. sanctions programs (e.g. North Korea), foreign subsidiaries owned or controlled by U.S. Persons also have U.S. compliance obligations.

For this reason, TELUS prohibits the involvement of U.S. Persons in its dealings (if any) with OFAC's "Embargoed Countries" (at the time of this Policy's release, OFAC's "Embargoed Countries" are Cuba, Iran, North Korea, the Crimea region of Ukraine, the Donetsk People's Republic and Luhansk People's Republic. This list is subject to change and team members must consult TELUS Legal for the current list of sanctioned countries.) and other OFAC sanctions targets unless OFAC has authorized or licensed such dealings. In addition, TELUS does not allow dealings with SDNs by either U.S. Person or non-U.S. Person TELUS team members.

Similarly, where EU or UK sanctions are applicable, TELUS prohibits the involvement of team members who qualify as EU or UK Persons, or whose activities involve an EU or UK nexus, in transactions which are prohibited under the respective EU or UK Sanctions.



vii. Records retention

TELUS will comply with the record retention requirements for all records compiled and maintained in accordance with the Sanctions Laws. All documents required to be maintained under U.S. sanctions laws must be maintained for a minimum of ten (10) years. Other jurisdictions may impose longer record retention periods - TELUS team members are responsible to determine if such longer retention periods apply.



viii. Training and education

TELUS provides integrity training on the TELUS Code of Ethics and Conduct to all TELUS team members, and team members are required to complete the training.

More in-depth training on Sanctions Laws is provided to TELUS team members, including those in departments that are identified as higher risk for a potential violation of Sanctions Laws, or have dealings in high-risk jurisdictions or have potential for direct or indirect contact with government officials. The training covers the processes and controls intended to mitigate the risk of a potential violation of Sanctions Laws, expectations of ethical conduct related to sanctions requirements and promotes a deeper understanding of sanctions related considerations.



ix. Guidance and reporting

If any TELUS team member knows, believes, or suspects that questionable, unauthorized, or illegal activities may have taken place in violation of applicable Sanctions Laws or this Policy (including any request from a third party to engage in such activities), they are required to report such activities to the [TELUS Ethics line](#).



x. Policy review

This Policy will be reviewed annually by the Chief Data & Trust Officer, who will recommend any material amendments to the Corporate Governance Committee of the TELUS Board. Amendments of a non-material nature may be approved by the Chief Legal and Governance Officer and the Chief Data & Trust Officer.



Appendix A: Red Flags of Potential Sanctions Evasion

- A business partner is unfamiliar to TELUS with minimal public track record;
- The business partner uses only a post office box address or is based in a secrecy jurisdiction for no apparent legitimate reason;
- The terms for financing the transaction or the price to be paid seem inconsistent with usual commercial standards;
- 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;
- A customer is reluctant to share information about the end use of a product, including reluctance to complete an end-user form;
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
- Declining customary installation, training, or maintenance of the purchased item(s);
- A customer's transactions are initiated from or sent to the following types of Internet Protocol ("IP") addresses: non-trusted sources; locations in high-risk jurisdictions and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious;
- IP addresses that do not correspond to a customer's reported location data;
- Last-minute changes to shipping instructions that appear contrary to customer history or business practices;
- Transactions involving entities whose website or business registration states the entities work on "special purpose projects";
- Payment coming from a third-party country or business not listed on the applicable end-user form;
- Use of personal email accounts instead of company email addresses; operation of complex and/or international businesses using residential addresses or addresses common to multiple closely-held corporate entities;
- Changes to standard letters of engagement that obscure the ultimate customer;
- Transactions involving a change in shipments or payments that were previously scheduled for a sanctioned jurisdiction;
- Transactions involving entities with little or no web presence;
- Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to sanctioned jurisdictions. Such locations may include China (including Hong Kong and Macau) and jurisdictions close to Russia or Iran, including Armenia, Turkey, and Uzbekistan;
- Multiple smaller transactions instead of one larger transaction without clear business justification, transaction amounts just below established screening or reporting thresholds, artificial segmentation of transactions across different departments or entities to avoid consolidated review;
- Customers requesting payment in cryptocurrency or through the use of cryptoexchanges or blockchain-based settlement methods; or
- Customers unable or unwilling to identify ultimate beneficial owners or ownership structure includes multiple layers across different jurisdictions or involves trusts, foundations, or anonymous mechanism.