

Politica in materia di sanzioni TELUS



Sommario

i.	Introduzione e finalità	3
ii.	Ambito di applicazione	4
iii.	Definizioni	5
iv.	Responsabilità	6
v.	Controlli di conformità	7
vi.	Isolamento e ricusazione di personale usa, ue e uk	8
vii.	Conservazione della documentazione	9
viii.	Formazione e aggiornamenti	10
ix.	Assistenza e segnalazioni	11
x.	Revisione della policy	12
	Appendice A: Indicatori di rischio (red flag) di elusione delle sanzioni	13

i. Introduzione e finalità

In TELUS, siamo fieri di posizionarci come leader mondiale nelle pratiche etiche aziendali. Il modo in cui lavoriamo è importante quanto ciò che facciamo. Il nostro obiettivo è dimostrare il massimo livello di etica e integrità in tutte le nostre relazioni con clienti, fornitori, istituzioni, membri del team e altri stakeholder. Questa responsabilità è condivisa da tutti i componenti del team TELUS e viene descritta nel dettaglio all'interno del nostro [Codice etico e di condotta](#).

Il rispetto delle normative sulle sanzioni internazionali consente di attenuare i rischi legali e le potenziali sanzioni pecuniarie. La conformità normativa valorizza la reputazione e la credibilità dell'azienda, consolidando la fiducia di clienti, partner e stakeholder. Tutela l'azienda da perdite finanziarie derivanti dal congelamento dei beni e da blocchi operativi che potrebbero derivare dall'interazione con entità sottoposte a sanzioni. Inoltre, un approccio proattivo alla conformità può garantire un vantaggio competitivo, in quanto testimonia l'impegno verso una condotta etica e una corretta gestione del rischio.

La finalità della presente Politica è definire il nostro approccio per garantire la piena conformità a tutte le sanzioni applicabili alle nostre attività aziendali e la corretta gestione dei rischi associati.



ii. Ambito di applicazione

La presente politica si applica a tutti i membri del team di TELUS e alle Terze parti.

Per i membri del team di TELUS: Tutti i membri del team di TELUS sono tenuti a prendere visione della presente Politica e a rispettarla in tutte le giurisdizioni in cui TELUS opera, nonché a effettuare verifiche e due diligence appropriate sulle controparti prima di avviare qualsiasi transazione o stipulare accordi. In caso di conflitto tra la presente Politica e la legge locale, si dovrà seguire lo standard previsto dalla Politica, anche qualora la legge locale consenta l'eventuale condotta in questione. Nel caso le leggi applicabili richiedano uno standard di condotta più stringente, sarà necessario attenersi a tale standard. Qualsiasi conflitto tra la presente Politica e le normative sulle sanzioni deve essere risolto a favore dello standard più stringente.

Per le Terze parti: Le Terze Parti devono soddisfare standard etici in linea con gli standard di settore e con la presente Politica, osservare tutte le leggi applicabili, incluse le normative sulle sanzioni, e astenersi da qualsiasi forma di aggiramento delle sanzioni stesse. Per quanto riguarda i fornitori di TELUS, essi devono inoltre attenersi alla Politica di Due Diligence per i fornitori di TELUS.

La presente Politica integra le altre politiche di TELUS correlate, tra cui la politica di Politica Anticorruzione e la Politica di Due Diligence per i fornitori di TELUS. In caso di incongruenza tra la presente

Politica e qualsiasi altro documento (inclusa qualsiasi istruzione di lavoro, procedura operativa standard o modulo), termini di quest'ultima prevarranno.

Il Chief Data & Trust Officer di TELUS è responsabile dell'applicazione della presente Politica con il supporto dell'ufficio legale di TELUS , al fine di assistere l'azienda e i membri del team di TELUS nel rispettare tali requisiti.



iii. Definizioni

Nel presente documento:

“Politica” indica la presente Politica

in materia di sanzioni “Parti soggette a restrizioni” indica:

- una persona fisica o giuridica iscritta dall’OFAC nell’elenco dei Specially Designated National (“SDN”) o altrimenti oggetto di sanzioni OFAC (ad esempio, un governo o un residente di un Paese sottoposto a embargo, oppure un’entità controllata al 50% o più da un SDN);
- una persona fisica o giuridica iscritta dal Dipartimento del Commercio degli Stati Uniti nell’elenco delle parti soggette a restrizioni sulle esportazioni statunitensi;
- una persona fisica o giuridica designata ai sensi delle normative sulle sanzioni dell’UE (inclusa qualsiasi persona fisica o giuridica inserita nell’elenco delle sanzioni dell’UE, o qualsiasi entità controllata al 50% o più, o altrimenti sottoposta al controllo di tale soggetto);
- una persona fisica o giuridica designata ai sensi delle normative sulle sanzioni dell’UK (inclusa qualsiasi persona fisica o giuridica inserita nell’elenco delle sanzioni dell’UK, o qualsiasi entità controllata, direttamente o indirettamente, da tale soggetto con una quota superiore al 50%);
- una persona fisica o giuridica designata come oggetto di sanzioni ai sensi delle leggi di altri ordinamenti in cui la Società opera

“Normative sulle sanzioni” indica tutte le leggi, gli statuti e i regolamenti applicabili in vigore al momento della transazione pertinente e relativi alle sanzioni economiche e commerciali imposte e gestite da qualsiasi autorità governativa o organizzazione internazionale, comprese quelle amministrate dall’Ufficio per le sanzioni di Global Affairs Canada, dall’Office of Foreign Assets Control (“OFAC”) del Dipartimento del Tesoro degli Stati Uniti, dal Dipartimento di Stato degli Stati Uniti, dal Consiglio di Sicurezza delle Nazioni Unite, dall’Unione Europea (“UE”) e dall’Office of Financial Sanctions Implementation (“OFSI”) del Regno Unito.

“Elenco SDN” indica l’elenco, pubblicato dall’OFAC, delle persone fisiche e giuridiche controllate o di proprietà di paesi sottoposti a sanzioni da parte dell’OFAC, o che agiscono per conto o per conto dei medesimi. Comprende, inoltre, individui, gruppi ed entità, come terroristi e narcotrafficienti, designati nell’ambito di programmi OFAC non legati a uno specifico Paese. Collettivamente, tali individui e società sono definiti “Specially Designated Nationals” or “SDN”.

“TELUS” indica TELUS Corporation o una qualsiasi delle sue controllate.

“Membri del team di TELUS”, o “membri del team”, indica gli amministratori, i dirigenti e i dipendenti di TELUS.

“Terze parti” indica tutti i soggetti e le entità esterni che agiscono per conto di TELUS (inclusi consulenti, appaltatori, fornitori e collaboratori commerciali in outsourcing).

“Soggetti Statunitensi” indica tutte le entità costituite secondo la legge degli Stati Uniti, tutti i soggetti presenti negli Stati Uniti e qualsiasi cittadino statunitense o titolare di green card statunitense.

iv. Responsabilità

Prima di effettuare qualsiasi transazione o stipulare accordi, i membri del team devono attenersi ai controlli e alle procedure predisposti da TELUS per garantire la conformità con le Normative sulle sanzioni. I membri del team devono inoltre prestare attenzione agli indicatori di elusione delle sanzioni, come quelli descritti nell'Appendice A. Qualora un membro del team ritenga che una transazione possa violare le Normative sulle sanzioni o che determinate azioni possano costituire un'elusione, deve sospendere la transazione e consultare immediatamente il proprio responsabile e il Dipartimento Legale di TELUS. La transazione o azione non deve riprendere l'approvazione scritta del Dipartimento Legale di TELUS e del Vicepresidente della relativa unità aziendale.



v. Controlli di conformità

Per garantire la conformità con le Normative sulle Sanzioni, TELUS ha predisposto una serie di controlli e procedure.

Tali controlli includono:

- verifiche e attività di due diligence sulle proprie controparti, quali clienti, fornitori, venditori e agenti, rispetto alle liste dei soggetti sottoposti a restrizioni (incluse quelle gestite dalle autorità statunitensi, dell'UE e del Regno Unito, come l'Elenco SDN degli Stati Uniti);
- divieto di porre in essere condotte volte o destinate a eludere o aggirare le Normative sulle Sanzioni;
- gestione e aggiornamento di un elenco dei "Paesi sottoposti a embargo";
- svolgimento di valutazioni del rischio ad hoc, ove richiesto, nelle regioni ad alto rischio e monitoraggio di processi e controlli specifici;
- in funzione della natura del rapporto, inserimento di obblighi di conformità alle sanzioni nei contratti commerciali stipulati con le controparti; e
- esecuzione di audit periodici sulla conformità alla presente Politica.

L'elenco sopra riportato non è esaustivo e TELUS si riserva la facoltà di adottare altri controlli e procedure che riterrà di volta in volta necessari.

Qualora una transazione o una relazione commerciale programmata debbano figurare come direttamente o indirettamente collegate a un Soggetto sottoposto a restrizioni, la transazione o la relazione potranno proseguire esclusivamente previa approvazione scritta da parte della Direzione Legale e di Governance di TELUS e del Vicepresidente responsabile dell'unità aziendale in cui è ha avuto origine la transazione.



vi. Isolamento e ricusazione di personale usa, ue e uk

Sebbene TELUS non sia un Soggetto Statunitense, tutti i suoi uffici e i membri del team di TELUS negli Stati Uniti, nonché qualsiasi membro del team di TELUS a livello globale che sia cittadino statunitense o titolare di green card statunitense, sono Soggetti Statunitensi. In assenza di una licenza, autorizzazione o esenzione applicabile, le Sanzioni Statunitensi vietano il coinvolgimento di Soggetti Statunitensi in operazioni con soggetti target delle sanzioni OFAC. Nel caso di determinati programmi di sanzioni statunitensi (ad es. Corea del Nord), anche le controllate estere di proprietà di, o controllate da, Soggetti Statunitensi hanno obblighi di conformità ai sensi della normativa statunitense.

Per tale ragione, TELUS vieta il coinvolgimento di Soggetti Statunitensi nelle proprie operazioni (ove presenti) con i “Paesi sottoposti a embargo” da parte dell’OFAC (al momento della pubblicazione della presente Politica, i “Paesi sottoposti a embargo” per l’OFAC sono Cuba, Iran, Corea del Nord, la regione della Crimea in Ucraina, la Repubblica Popolare di Donetsk e la Repubblica Popolare di Luhansk. Il presente elenco può subire modifiche e i membri del team devono consultare l’Ufficio Legale di TELUS per conoscere l’elenco aggiornato dei Paesi sanzionati) e con altri soggetti target delle sanzioni OFAC, a meno che l’OFAC non abbia autorizzato o concesso apposita licenza per tali operazioni. Inoltre, TELUS non consente relazioni commerciali con soggetti SDN da parte dei membri del team di TELUS, siano essi Soggetti Statunitensi o no.

Analogamente, laddove siano applicabili le sanzioni dell’UE o del Regno Unito, TELUS vieta il coinvolgimento dei membri del team definiti come Soggetti dell’UE o del Regno Unito, o le cui attività comportino un elemento di collegamento con l’UE o con il Regno Unito, in operazioni vietate ai sensi delle rispettive Sanzioni dell’UE o del Regno Unito.



vii. Conservazione della documentazione

TELUS si adeguerà ai requisiti di conservazione dei documenti per tutte le registrazioni raccolte e mantenute in conformità con le Normative sulle Sanzioni. Tutti i documenti di cui è richiesta la conservazione ai sensi delle normative statunitensi sulle sanzioni devono essere conservati per un periodo minimo di dieci (10) anni. Altri ordinamenti giuridici possono imporre periodi di conservazione più lunghi; sarà cura dei membri del team di TELUS stabilire l'effettiva applicabilità.



viii. Formazione e aggiornamenti

TELUS eroga una formazione sull'integrità relativa al Codice Etico e di Condotta di TELUS e tutti i membri del team di TELUS sono tenuti a completarla.

Una formazione più approfondita sulle Normative sulle sanzioni viene erogata ai membri del team di TELUS, inclusi coloro che operano in dipartimenti considerati a maggior rischio di potenziale violazione delle Normative sulle sanzioni, o che svolgono attività in ordinamenti ad alto rischio o che presentano un potenziale contatto diretto o indiretto con funzionari di governo. La formazione illustra i processi e i controlli volti a mitigare il rischio di una potenziale violazione delle Normative sulle sanzioni, le aspettative in materia di condotta etica legate ai requisiti sulle sanzioni e promuove una comprensione più approfondita delle valutazioni e implicazioni in materia di sanzioni.



ix. Assistenza e segnalazioni

Qualora un membro del team di TELUS sia a conoscenza, ritenga o sospetti che si siano verificate attività dubbie, non autorizzate o illecite in violazione delle Normative sulle sanzioni applicabili o della presente Politica (inclusa qualsiasi richiesta da parte di terzi di porre in essere tali attività), è tenuto a segnalare tali attività alla linea [Etica di TELUS](#).



x. Revisione della policy

La presente Politica è soggetta a una revisione annuale da parte del Chief Data & Trust Officer, il quale raccomanderà le eventuali modifiche sostanziali al Comitato per la Corporate Governance del Consiglio di Amministrazione di TELUS. Le modifiche di natura non sostanziale potranno essere approvate dalla Direzione Legale e di Governance e dal Responsabile Data & Trust.



Appendice A: Indicatori di rischio (red flag) di elusione delle sanzioni

- Un partner commerciale sconosciuto a TELUS che disponga di uno storico pubblico limitato;
- Un partner commerciale che utilizzi esclusivamente un indirizzo di casella postale o abbia sede legale in una giurisdizione che garantisce il segreto societario/bancario senza un'apparente ragione legittima, oppure;
- Delle condizioni di finanziamento di una data operazione o il prezzo da corrispondere che sembrano incoerenti rispetto ai consueti standard commerciali;
- Utilizzo di veicoli societari (ad esempio enti giuridici, quali società schermo, e istituti giuridici) per occultare (i) la proprietà, (ii) la provenienza dei fondi, o (iii) i Paesi coinvolti, con particolare riferimento alle giurisdizioni sottoposte a sanzioni;
- Rifiuto o reticenza del cliente a condividere informazioni sull'impiego finale di un prodotto, compresa la mancata compilazione del modulo per l'utilizzatore finale;
- Utilizzo di società schermo per effettuare bonifici internazionali, che coinvolgano istituti finanziari ubicati in giurisdizioni diverse da quella di registrazione della società;
- Rifiuto delle normali attività di installazione, formazione o manutenzione degli articoli acquistati;
- Esecuzione di transazioni da parte del cliente provenienti da, o indirizzate alle seguenti tipologie di indirizzi IP: fonti non attendibili; località situate in giurisdizioni ad alto rischio o sottoposte a sanzioni globali; oppure indirizzi IP precedentemente segnalati come sospetti;
- Indirizzi IP non corrispondenti ai dati di localizzazione dichiarati dal cliente;
- Modifiche dell'ultimo minuto alle istruzioni di spedizione che appaiano contrarie allo storico o alle pratiche di business del cliente;
- Esecuzione di operazioni che coinvolgano enti la cui registrazione societaria o il cui sito web indichino che essi operano su "progetti a scopo speciale";
- Pagamenti provenienti da un Paese terzo o da un'impresa non indicati nel relativo modulo per l'utilizzatore finale;
- Utilizzo di account di posta elettronica personali al posto di indirizzi e-mail aziendali; gestione di attività d'impresa complesse e/o internazionali tramite indirizzi residenziali o indirizzi condivisi da più entità societarie a ristretta base azionaria;
- Modifiche alle lettere di incarico standard volte ad occultare il cliente finale;
- Operazioni che comportino una variazione delle spedizioni o dei pagamenti precedentemente programmati verso una giurisdizione sottoposta a sanzioni;
- Operazioni che coinvolgano organizzazioni con una presenza sul web ridotta o del tutto assente;
- Instradamento degli acquisti attraverso determinati punti di trasbordo comunemente utilizzati per reindirizzare illegalmente beni soggetti a restrizioni verso Paesi o territori sottoposti a sanzioni. Tali località possono includere Cina (comprese Hong Kong e Macao) e Paesi limitrofi a Russia o Iran, tra cui Armenia, Turchia e Uzbekistan;
- Esecuzione di più operazioni di importo ridotto al posto di un'unica operazione di importo maggiore in assenza di una chiara giustificazione commerciale; frazionamento di importi al di sotto delle soglie stabilite per il controllo o la segnalazione; segmentazione artificiosa delle operazioni tra diversi dipartimenti o entità per evitare una revisione consolidata;
- Richiesta da parte del cliente di effettuare i pagamenti in criptovalute oppure tramite l'uso di piattaforme di scambio di criptovalute o sistemi di regolamento basati su tecnologia blockchain;
- Impossibilità o rifiuto da parte del cliente a identificare i titolari effettivi, oppure presenza di assetti proprietari con catene di controllo multilivello diffuse in più Paesi, o basate su trust, fondazioni o strumenti anonimi.