Catena
Inspection & Engineering Services Ltd
Lifting Solutions & Supplies

CHR029 Sanctions Policy and Procedure

MAY 2025 | ISSUE 1

What is a Sanction?

Sanctions are political and economic measures used as a foreign policy tool by governments and the international community to try to influence the behaviour of other governments, businesses and individuals. In some cases, sanctions may be applied indiscriminately to entire countries or regions, but in most cases, they are applied on a more targeted basis to specified individuals, businesses and other organisations.

Breaches of sanctions law carry a risk of serious penalties for both organisations and individuals, as well as the risk of negative publicity and serious reputational damage. Penalties can be criminal, including unlimited fines and imprisonment.

Catena has adopted this Sanctions Policy and will operate management processes to ensure that the company and its employees can appropriately manage the risk of becoming affected by sanctions or sanctions breaches.

As a starting point, the companies aim will always be to avoid engaging in business which contravenes any applicable sanctions laws. Catena will also seek to require its third-party service providers, suppliers and other relevant trading partners to comply with the companies aim.

This Policy sets out key principles designed to ensure that all of us can comply with all applicable sanctions regimes and avoid the potentially serious consequences for Catena and individuals that can flow from any breach of sanctions.

All Catena employees are required to comply with this Sanctions Policy at all times. Non-compliance with this Sanctions Policy by Catena employees will be addressed in accordance with the companies disciplinary procedures and local law. Catena may require its third-party service providers and other suppliers to commit to comply with this Sanctions Policy. Failure to do so may trigger serious consequences, including the termination of relevant contracts and trading relationships, and certain breaches of this Sanctions Policy may constitute violations of laws, which may result in legal action in accordance with applicable laws and contractual agreements.

All Catena employees are expected and required to report any circumstances, knowledge or suspicions of non-compliance with this Sanctions Policy or any known or suspected breach of applicable sanctions laws. Reports should be made directly to the IMS Manager (k.moss@catenais.co.uk)

All reports will be promptly and thoroughly investigated. All matters will be dealt with in confidence, protecting the rights of individuals and respecting applicable laws.

Any non-urgent questions in relation to this Sanctions Policy should also be directed to the IMS Manager.

Procedure

Often, the most significant and obvious risk factor in relation to Sanctions is the country. In some cases, a counterparty may not itself be located or operating in a high-risk country, but it may become known to you that it is owned or controlled by, or acting on behalf of, a person, organisation or governmental body in a high-risk country.

There are a small number of countries which pose a high risk from a Sanctions perspective and for these countries our policy is that no member of Catena should engage in business relationships, transactions or other dealings that involve counterparties in those countries.

If you come across a transaction or relationship that you know or suspect to involve any of these high-risk countries, you should stop that activity and immediately notify the IMS Manager or Managing Director.

There are also a number of medium-risk countries with which business may be permitted, but for which detailed review will be required before any commitment may be given by or on behalf of any employee of Catena.

Conducting business in, or with parties connected to, the following "**high-risk**" countries / territories is likely to be complex to navigate in compliance with applicable Sanctions. Therefore, the general rule is that **no Employee or Relevant Third Party should make or agree arrangements or business in, with or in connection with the following countries**.

High-risk countries:

the Republic of Belarus; Crimea, Sevastopol, Luhansk, Donetsk, Kherson and Zaporizhzhia (disputed regions of Ukraine); Cuba; Iran; North Korea (DPRK); Russia; Syria; and Venezuela.

Please be aware that all transactions or business relationships involving Russia, Belarus or the sanctioned regions of Ukraine are prohibited.

Medium-risk countries:

Afghanistan; Armenia, Azerbaijan, Burma/Myanmar; Burundi, the Central African Republic; the Democratic Republic of the Congo; Guatemala; Guinea; the Republic of Guinea-Bissau; Haiti; Iraq; Lebanon; Libya; Maldives; Mali; Nicaragua; Palestinian Territories; Somalia; South Sudan; Sudan; Tunisia; Ukraine; Yemen; and Zimbabwe.

The following jurisdictions are common "**Diversion Hubs**" for the evasion of Sanctions targeted at Russia and Belarus. It is not prohibited to engage in business relationships and transactions in these territories. However, you should apply additional scrutiny and look out for any "**red flags**" which may indicate that a counterparty is using a Diversion Hub to evade Sanctions targeted at Russia or Belarus. These include the non-exhaustive list of behavioural "red flags" set out in the box below, which are particularly prevalent in the circumvention of Sanctions against Russia and Belarus, but may also be "red flag" indicators of potential Sanctions breaches in other contexts.

• A customer requests delivery to a free trade zone, freight forwarder or ship **without any further details on destination**.

• A customer requests delivery to a **different country from where they are located**, without good reason.

• An **unusual shipping route** is requested.

• **Last minute changes** to the transaction and / or agreement.

• A customer is **unusually evasive** about standard questions concerning delivery or KYC.

• A customer refuses to agree with **sanctions compliance contractual clauses**.

• A **lack of transparency over the counterparty's ownership structure and operations** (e.g., a refusal to provide information on ownership, little or no online presence).

• A customer attempts to **conceal the involvement of third parties**.

• A customer is a **shell company** with no apparent physical assets.

• A customer uses other **complicated structures to conceal involvement**, for example layered letters of credit, front companies or unusual intermediaries / brokers.

• A customer does not operate in an industry sector that would **typically require or purchase Catena products**.

• A customer proposes that payment be made by a **different entity**.

• A customer proposes that payment be made through **multiple intermediary banks**.

• A customer offers **unusual payment amounts or terms**, without good reason.

• **Use of Russian language** in communications and / or commercial agreements.

Diversion Hubs:

Afghanistan; China; Cyprus; Faroe Islands; Georgia; Jordan; Kazakhstan; Kuwait; Kyrgyzstan; Malaysia; Mongolia; Panama; Pakistan; Qatar; Saudi Arabia; Tajikistan; Thailand; Turkey; Turkmenistan; United Arab Emirates; and Uzbekistan.

If you know or suspect that any counterparty is deliberately trying to evade Sanctions targeted at Russia or Belarus, or if you identify any red flags involving a Diversion Hub, you should stop that activity and notify the IMS Manager or Managing Director.