NORTH DATA

Risk Signals

Sanctions

Ownership & Control Risk Signals

The “February 2022” Ownership Shift

- Russian Ultimate Beneficial Owners (UBOs) of EU-based companies faced increased pressure after February 2022, and ownership changes around sanction packages may warrant scrutiny.
- Use North Data to identify companies owned or managed by Russian or Belarusian individuals prior to early 2022, or shortly before relevant EU sanctions. Watch for transfers of these companies to local nationals, third-country proxies, or holding companies in jurisdictions such as Cyprus or the UAE. These patterns warrant follow-up but are not, on their own, proof of evasion.
- Sometimes, an ownership transfer is just for show. The new owner acts as a figurehead, while the original sanctioned owner still secretly controls the business using legal loopholes, hidden contracts, or a Power of Attorney. Registry data alone cannot prove evasion or continued control.

Cross-Referencing against Domestic Sanctions Lists

- Individual member states often maintain their own public national sanctions list targeting specific individuals and companies supporting the Russian Federation (independent of the broader EU list).
- Take the names of local directors, UBOs, and historic shareholders uncovered in North Data and cross-reference them with these lists.

Cross-Border / Trade Route Risk Signals

The Central Asian / Eurasian Detour

- Direct trade between Russia and the EU is heavily restricted. Risk patterns include paperwork routed through third-country jurisdictions commonly used for re-export: EAEU members (Russia, Armenia, Belarus, Kazakhstan, Kyrgyzstan) and other neighboring or hub jurisdictions such as Uzbekistan, Georgia, Turkey, and the UAE.
- How to spot it via North Data: Look at the network graph. Sanctions-circumvention schemes frequently use intermediate shell companies in these jurisdictions. Investigations and enforcement reports have documented cases in which the country of origin of goods was misdeclared, for example as Kazakhstan, to evade restrictions. Confirming this requires customs and shipping records, not registry data alone.

Geographic Clustering

- Geography matters immensely in supply chain fraud. A company's registered address can tell you if it is positioned to exploit physical border crossings.
- The Infrastructure Mismatch: Be highly suspicious of companies registered in high-risk Eastern border regions (such as those bordering Russia, Belarus, or Ukraine) that declare millions in turnover but have no visible physical infrastructure, like yards, trucks, or warehouses. This mismatch warrants immediate verification against shipping and customs evidence.
- The Logistics Hub Check: Look for companies registered near major rail or port transshipment hubs. If a newly formed company with zero history is suddenly handling heavy freight traffic through these border nodes, it requires deep scrutiny.

Financial & Business Activity Risk Signals

Sudden Industry Shifting

- Companies within the EU register their specific business activities using NACE classification codes.
- Watch for companies that historically operated in genuinely domestic, low-risk sectors (e.g. local retail, catering, or facility maintenance) suddenly expanding their field of activity or stated corporate purpose to include the wholesale of restricted goods such as timber, coal, scrap metal, or electronic components. These commodities are targeted by international import bans and dual-use export controls.
- This is a potential sign that the business has been acquired or repurposed. Additional fact-finding and due diligence would be beneficial.

Contact Information

www.northdata.com

welcome.northdata.com/en/newsletter

info@northdata.com

/company/northdata

blog.northdata.com

christina.brause@northdata.com