BLOMSTEIN

Sanctions 101

A Survival Guide for IT and Software Companies

12 September 2024

Over the summer, not only the EU has tightened its sanctions against Russia and Belarus (see our previous briefings here and here). The US has also imposed additional restrictions with a particular focus on certain hardware, software, and services (see, e.g., here and here). However, many of these new US restrictions have been part of the EU sanctions in one form or another for some time now. Still, it is often overlooked that these restrictions have a significant impact on IT and software products and can affect business relationships with customers outside of Russia and Belarus.

It is important that companies, not just those based in the EU, assess whether they are affected by EU sanctions. While any EU person or company must comply with EU restrictive measures wherever they operate, non-EU companies may also be subject to EU restrictive measures. This is the case if they operate from within the EU or if individual transactions are at least partly done in the EU (see Article 13 of Regulation (EU) No 833/2014, as amended (***Regulation 833/2014***) and Article 10 of Regulation (EC) No 765/2006, as amended (***Regulation 765/2006***)). The mere existence of servers located in the EU may not be sufficient to trigger the application of EU sanctions law. But if there are other connecting elements, third-country companies should be wary of the application of EU sanctions law and closely analyse the following restrictions in particular:

- Prohibitions apply to the sale, supply, transfer and export of a **wide range of hardware** to anyone or for use in Russia and Belarus. This includes, e.g., encryption equipment, servers, computers, laptops, and electronic components (see Articles 2, 2a, and 3k Regulation 833/2014 and Articles 1e, 1f, and 1bb Regulation 765/2006).

- Trade restrictions also apply to specific **software**. Importantly, these restrictions concern not only the export of such software, but also other forms of provisioning, including the granting of access through cloud platforms. These restrictions concern:

    - **Dual-use software** under Dual-use Regulation (EU) 2021/821, as amended, such as software with encryption functionality controlled as 5D002 (which correlates with ECCN 5D002 under US export control law) (see Article 2 Regulation 833/2014 and Article 1e Regulation 765/2006),

    - **mass-market encryption software**, classified under US law as ECCN 5D992, which encompasses several off-the-shelf software products (see Article 2a of Regulation 833/2014 and Article 1f Regulation 765/2006),

  - **enterprise management software** and **industrial design and manufacture software**, which covers a wide range of software products, such as enterprise resource planning, customer relationship management, supply chain management or enterprise data warehouse software as well as, for example, computer-aided design or engineer-to-order software (see Article 5n (2b) Regulation 833/2014 and Article 1jc (4) Regulation 765/2006).

- Restrictions are also imposed on the provision of IT services, namely

  - **technical assistance and other services** related to sanctioned software or hardware (which may include after-sales services for software provided to Russian or Belarussian customers prior to the Russian aggression) and

  - **IT consultancy services**, covering a wide array of activities, such as consultancy related to the installation of computer hardware or to the development and implementation of software (see Article 5n (2) Regulation 833/2014 and Article 1jc (2) Regulation 765/2006).

The **scope of these prohibitions** is not uniform and requires close legal analysis. For example, the prohibitions on hardware and encryption software concern transactions with anyone or for use in Russia or Belarus. In contrast, the prohibitions on enterprise management software and IT consulting services apply only with respect to the Russian government and Russian companies, whereas, in case of Belarus, the scope is primarily limited to Belarussian public entities as well as to persons acting on behalf of or at the direction of such entities. The relevant exemptions and the ability to obtain an authorisation from the relevant authorities also differ depending on the prohibition in question.

An important element common to all prohibitions is that they cover not only direct but also **indirect constellations**. Thus, the supply of software to non-Russian and non-Belarussian third-country or even EU customers may be restricted if the hardware, software or service is subsequently made available to restricted recipients in Russia or Belarus. Companies should therefore ensure that their direct customers do not provide access to their products and services from these countries. They should be particularly sensitive if their direct customers have customers or subsidiaries in Russia or Belarus, or are themselves subsidiaries of a Russian or Belarusian parent. In such a case, operators should make sure that their products or services do not (also) benefit a company based in Russia or Belarus. It is advisable to address this issue contractually and, depending on the risk profile of each case, to put in place technical safeguards such as geofencing.

At BLOMSTEIN, we have extensive experience in assisting EU and non-EU IT and software companies navigate the EU restrictions. Please do not hesitate to contact Florian Wolf or Tobias Ackermann, who will be happy to assist you with your questions.

***