Patrick Goergen Apr 28, 2021 1 min read

UK issues new guidance on tangible and intangible transfer of dual-use and military technology

Technology transfer is among the most critical issues of any export control compliance policy. It touches daily tasks as well as strategic decisions.

How to use for example USB flash drives, laptops and tablets? What are precautions to take by doing phone calls or video-conferencing? What appropriate actions to take to insure that information in an email is suitably protected (think about automatic email forwarding to addresses abroad) ?

What about transfers within multinational companies, who are sharing common IT systems? What about employees travelling abroad with controlled technology stored on company or personal devices?

And then cloud storage and routing. Does it make a difference where the servers containing the controlled technology are located? Or is only the location of the exporter and the intended recipient relevant? How to protect information when uploading controlled technology to or through the cloud? What safeguards to use? What about third party access to intranets or cloud services? And if an entity located abroad is doing IT system testing and maintenance?

What are the correct definitions of information that is in "the public domain" and of "basic scientific research"?

The Guidance is full of practical examples and case studies and provides a good base for internal policies.

Source: UK Guidance (22 Mar 2021)