China state-controlled nuclear company pleads guilty to illegal exports to Pakistan 2

U.S. satellite industry receives ITAR relief 2

UK government imposes new restrictions on financing Iran transactions 6

Germany debates new export control law 14

Cloud computing and EU export controls compliance 16

The Slovak Republic’s export control regime 19

Out of Mexico: a step-by-step guide to compliant exporting 22

Export controls South Korea-style 26
Cloud computing and EU export controls compliance

Cloud computing can throw up a whole host of export control issues. Sajid Ahmed and Dr. Philip Haellmigk detail the questions that EU-based persons who wish to take advantage of cloud computing’s benefits while complying with export controls should ask.

A major regulatory challenge posed by cloud computing is how to ensure that software/technology transmitted to a ‘cloud’ does not fall foul of any potential EU/Member State export controls legislation.

Just because the principals involved in a cloud computing transaction are domestic companies, it does not necessarily mean there is no ‘export’ when a transmission of software/technology takes place. For instance, if a UK company stores data via the Internet on a remote server owned by another UK company but located in India, then from an EU export controls standpoint an export takes place when the data is transmitted from the UK to India i.e., a destination outside the EU. The fact that the two principals in this transaction are UK companies is irrelevant for the purposes of export controls – what matters is whether there has been a cross-border transmission of data (i.e., outside of the EU).

Unfortunately, the EU authorities have so far not provided any formal guidance on export controls in the context of cloud computing. In the U.S., the Department of Commerce has published a couple of advisory opinions which deal with, among other things, whether or not a cloud computing service can be regarded as an export.

Unlike in the U.S., where experts have extensively commented on these Department of Commerce advisory opinions, not much has been written about cloud computing and EU export controls. In this article, we provide some practical questions companies in the EU involved in cloud computing, either as users or providers, should be asking themselves.

This article only focuses on EU/Member State export controls legislation – depending upon the fact pattern, EU/Member State sanctions legislation or export controls/sanctions legislation of other countries such as the U.S. should also be considered.

Is the software/technology controlled? What cloud options are available?

Obviously, if the concerned software/technology is not controlled then there is no need to worry about export controls. If, however, the software/technology is controlled then the focus should be on what options are available to reduce the compliance burden.

If the controlled software/technology is stored on servers in non-EU destinations, it is critical to determine the route of the transmission.

For instance, can the service be provided domestically i.e., within the relevant Member State and on a private cloud where the cloud is built exclusively for the user and the route and server are self-contained within the Member State? If this can be achieved, then there will be no export of the software/technology and hence, no compliance burden. This option could also be available for transmissions from one Member State to another; however, in some instances a licence may be required for intra-EU transmissions.

Another option to consider is whether the controlled part of the software/technology can be separated from the rest of the item and if so, is it possible to restrict the use of the cloud-computing service to the non-controlled part of the software/technology? If this is feasible and the controlled part of the software/technology is not exported, then there would be no compliance burden.

What is the route of the transmission? Who will have access to the controlled software/technology? What will be done to the software/technology when accessed?

If the controlled software/technology is stored on servers in non-EU destinations, it is critical to determine the route of the transmission. For instance, if controlled data is being transmitted from the UK to Malaysia, it may not be as simple as seeking an export licence from the UK authorities. It may be that the transmission is routed to Malaysia via Singapore, in which case one has to determine whether or not an export licence from the Singapore authorities is also required.

Furthermore, it is important to find out who will have access to the controlled data. Even if the data is stored in a country which is not subject to sanctions (such as Singapore), the individuals who have access to the server in Singapore (via the Internet) may themselves be subject to sanctions or located in countries subject to sanctions. Accordingly, it is important to list and screen all personnel who will have access to the controlled data. (It is important to highlight that unlike in the U.S., in the EU there is typically no ‘deemed export’ concept and hence, there should be no export controls exposure for domestic transmissions involving foreign nationals.)

It will also be vital to understand whether there will be repeated uploads/downloads and, if so, will there be any modifications to the controlled software/technology. The former will help to determine the type
of export licence required; e.g., if there are many emails with the controlled data attached, then a licence covering multiple transmissions should be sought. In relation to the latter, if there are any meaningful modifications to the concerned software/technology, a new/amended licence may be needed before the software/technology can be re-transmitted.

Who has the responsibility to comply with EU/Member State export controls legislation?
This is a critical issue for both the user and provider as non-compliance with EU/Member State export controls legislation can result in criminal liability. Normally, it is the exporter who has the burden of export controls compliance e.g., seeking an appropriate export licence.

The EU Dual-Use Regulation defines an 'exporter' as the person who decides to transmit or make software/technology available to a non-EU destination. Based on this definition, in the context of cloud computing it is the user that decides to transmit or make available any software/technology because it is the user who chooses what to upload, determines when to do so, and lists who to provide access to.

The provider merely supplies a network infrastructure and/or a development platform. The provider does not make any decisions about what software/technology should be transmitted or made available (except to the extent such software/technology belongs to the provider e.g., set-up/maintenance/trouble-shooter services).

Accordingly, under EU law it would appear that it is the user who is the exporter and, therefore, it is the user who has the burden of ensuring export controls compliance.

In the U.S., the Department of Commerce has stated that the cloud provider is not the exporter of the software/technology, thereby suggesting that the user has the responsibility of export controls compliance. This is consistent with the U.S. approach of applying the concept of 'common carriers' to telecoms operators. However, there is no similar formal guidance in the EU, causing some commentators to suggest that it would be sensible for both the provider and user to seek export licences when transmitting controlled software/technology.

While this may sound like an overly safe approach, it results in unnecessary duplication with scope for potential inconsistencies between the licence submissions. We would, therefore, recommend that in the first instance, a clarification be sought from the relevant EU Member State authority. If the authority fails to provide a clear steer on who should apply for the export licence then, depending upon the risk appetite of the partners, the options available are either the user apply only (based on the rationale provided above) or both the user and the provider seek such a licence.

---

**Case study: exporting to the cloud?**

'A' is a UK-based company that manufactures and supplies electronic devices, including recording equipment. One such recording equipment is an analogue instrumentation magnetic tape recorder with a bandwidth exceeding 4 MHz per electronic channel. Due to these characteristics, this tape-recorder is a controlled item as per the EU Dual Use Regulation. The technology for the production of such tape recorders is also controlled.

To date, A's manufacturing facilities are based in the UK (i.e., within the EU). It also has offices in Singapore (i.e., outside of the EU) but this is only a marketing office. At present, any export as such, occurs from the UK. A is aware that this item is controlled and, therefore, has obtained export licences from the UK Export Control Organisation ('ECO') for the export of these goods to third countries.

A's management board has now decided that the concerned tape-recorders should also be manufactured in Singapore to serve the growing demand in its Asia markets. Therefore, A intends to set up a private cloud allowing, among other things, its employees in Singapore to have access to the controlled manufacturing technology.

The cloud computing provider that A intends to use is a German company whose servers are based in Germany. A believes that it does not require an export licence with respect to the manufacturing technology that will be put on a cloud because (1) it is an intra-company transfer of technology; (2) the cloud computing provider is an EU company; and (3) there is no export of the technology to outside of the EU as A is uploading the controlled technology to a server located in the EU i.e., Germany.

A's view is incorrect. It will have to seek an export licence for its employees in Singapore to gain access to the controlled manufacturing technology. This is for the following reasons:

- Any cross-border transfer of controlled technology regardless of whether or not it is intra-company transfer is subject to export control rules.
- The nationality of the cloud computing company is irrelevant. What matters is whether there is an export.
- A wrongly assumes that access by employees outside the EU i.e., in Singapore to a server based in the Germany does not amount to an ‘export’. This is because the EU Dual Use Regulation provides that an ‘export’ also includes making available in an electronic form technology to persons outside the EU.

Accordingly, giving access to the controlled technology on a private cloud to A's employees in Singapore will be regarded as an export of controlled technology. A will therefore have to explore licensing requirements from the ECO, as well as the German authorities, Bundesamt für Wirtschaft und Ausfuhrkontrolle ('BAFA') given that the servers are based in Germany.

---

Conclusion
It is highly likely that an EU authority will publish some formal guidance on cloud computing and export controls in the near future. In this guidance, it is likely they will address the question whether it is the provider or user who has the responsibility of EU export controls compliance. This is one of the first questions the Department of Commerce in the U.S. addressed in its advisory opinions and we expect the guidance from the EU authorities in this respect to be similar to that provided by the Department of Commerce: i.e., it is not the provider who bears export controls compliance responsibilities.

In the meantime, it is advisable for companies in the EU involved in cloud computing, either as users or providers, to develop an internal export controls compliance programme – this is critical because notwithstanding the lack of EU guidance, cloud computing can entail cross-border transmission of software/technology which will result in exposure to export controls legislation if the subject software/technology is controlled.

Links and notes
1 Based on the UK Export Control Order 2008 ‘Technology’ is defined as information (including but not limited to information in software and documents such as blueprints, manuals, diagrams and designs) that is capable of use in connection with the development, production or use of any goods.
2 Each EU Member State is required to adopt and enforce EU export controls legislation i.e., Council Regulation 428/2009 (in conjunction with Council Regulation 388/2012). This legislation applies not only to EU nationals/companies but also to non-EU nationals/companies who conduct business in the EU. Some EU Member States, like the UK, have supplemented to these EU rules. For instance, the UK has additional export controls legislation against Iran. These additional rules normally apply to UK nationals/companies as well as foreign nationals/companies operating in the UK.
3 See http://www.bis.doc.gov/policiesandregulations/advisoryopinions.htm
4 Council Regulation 428/2009 (in conjunction with Council Regulation 388/2012) as well as Member State legislation that supplements EU law should be considered when determining what ‘dual-use’ software/technology is controlled. Consideration should also be given to Member State military control lists which sets out the list of military items (including software/technology) controlled.
5 It is still important to consider whether or not the person who has access to the software/technology is subject to sanctions or operates from a sanctioned country.
7 An export of software/technology is ‘deemed’ to take place when it is released to a foreign national within the US. See http://www.bis.doc.gov/deemedexports/deemedexportsfaqs.htm#1
8 Enforcement is carried out at Member State level. In the UK, a person found guilty of an export controls violation can face up to 7 years in prison and/or a significant fine.
9 See Article 2(3) of Council Regulation 428/2009 (in conjunction with Council Regulation 388/2012).
WorldECR

The journal of export controls and compliance

Contributors in this issue
Dr Bärbel Sachs, Noerr LLP
www.noerr.com
Sajid Ahmed and Dr. Philip Haellmigk, Bird & Bird LLP
www.twobirds.com
Eva Nagyová, Ružička Csekes s.r.o. in association with members of CMS
www.rc-cms.sk
Horacio A. López-Portillo, Vázquez Tercero & Zepeda
www.vazqueztercero.com
George Tan and Tatsuya Kanemitsu, Bryan Cave International Trade
www.bryancave.com

WorldECR Editorial Board
Michael Burton Arent Fox LLP, Washington DC.
burton.michael@arentfox.com
Larry E. Christensen, Miller & Chevalier, Washington DC.
lchristensen@milchev.com
ian.macvay@twobirds.com
Dr. Bärbel Sachs, Noerr, Berlin.
bärbel.sachs@noerr.com
Iain Sandford, Minter Ellison, Canberra.
iain.sandford@minterellison.com
Edmund Sim, Appleton Luff, Singapore.
sim@appletonluff.com
George Tan, Bryan Cave Consulting, Singapore.
george.tan@bryancave.com

General enquiries, advertising enquiries, press releases, subscriptions: info@worldecr.com
Contact the editor, Tom Blass: tnb@worldecr.com tel +44 (0)7930405003
Contact the publisher, Mark Cusick: mark.cusick@worldecr.com tel: +44 (0)7702289830

WorldECR is published by D.C. Houghton Ltd.
Information in WorldECR is not to be considered legal advice. Opinions expressed within WorldECR are not to be considered official expressions of the publisher. The publisher assumes no responsibility for errors and omissions appearing within. The publisher reserves the right to accept or reject all editorial and advertising matter. The publisher does not assume any liability for unsolicited manuscripts, photographs, or artwork.
© D.C. Houghton Ltd 2012. All rights reserved. Reproduction in whole or in part of any text, photograph, or illustration without express written permission of the publisher is strictly prohibited.
ISSN 2046-4797. Refer to this issue as: WorldECR [0208]

Correspondence address: D.C. Houghton Ltd, Suite 17271, Lower Ground Floor, 145-157 St John Street, London EC1V 4PW England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 145 - 157 St John St, EC1V 4PY, London, UK

ISSUE 18. DECEMBER 2012
www.WorldECR.com