UK Export Controls on Encryption Products

A legal update from Dechert's International Trade and EU Law Practice

September 2016
UK Export Controls on Encryption Products

Data protection, cybersecurity, commercial confidentiality and personal privacy all demand high standards of security. The main means to achieve this is by encrypting the data. But the hardware or software for doing this can be misused (highlighted by pressure from law enforcement agencies to have greater access to encrypted data to prevent and investigate terrorist attacks). The export of many such products is therefore subject to licensing. Although the rules are essentially the same across the EU and in the US, their interpretation varies widely and many businesses struggle to implement them correctly. With the anticipated European Commission amendment to the EU Dual-Use Regulation, we look at what is controlled, what is exempt, what licences are available and what is changing.

What Is Controlled?

Current EU and US regulations control most products capable of encryption (‘cryptographic products’). Strictly, the controls apply to those using symmetric algorithms with a key length over 56 bits or asymmetric algorithms with a key length over 512 bits, but in practice most commonly-used encryption protocols use key lengths exceeding these levels (e.g. AES 128, 1024 RSA and 1024 DH) so are subject to the regulations.

The controls are not restricted to hardware but include components, software and technology such as design data. Software or technology that is carried or transmitted outside the EU (e.g. sent by email or by remote access of a server) is also subject to control.

All information security items subject to export controls in the EU are listed in Category 5 Part 2 of Annex I of the EU Regulation 428/2009 (‘the Regulation’). All items on the list require a licence for export outside the EU unless they qualify for an exemption.

What is Exempt?

The regulators recognize that due to rapid advances in consumer technology, cryptographic products that only a few years ago were reserved for only the most sophisticated commercial users and government agencies are now commonplace on every smartphone and wireless router. In order to enable unrestricted trade in the highly-competitive market for such products, while retaining effective control of more sensitive items, the regulations allow for significant exemptions. These fall under seven main headings:

1) software ‘in the public domain’ i.e. software that has been made available without restriction (excluding copyright restrictions) upon its further dissemination. This generally exempts open source software, including that which is made available under a licence from the copyright holder;

2) products whose sole function is authentication, digital signatures or the execution of copy-protected software. This includes smart cards and their reader/writers if they are specially designed to protect personal data;

3) commonly-used commercial cryptographic equipment including that used for banking or money transactions; most civil mobile phones; cordless phones; short range wifi equipment; civil Radio Access Network equipment; routers, switches and relays limited to operations, administration or maintenance functions; and general purpose computing equipment and servers using only published or commercial cryptographic standards;

4) items accompanying their user for the user’s personal use;

5) goods that can be purchased by the general public without restriction from retail selling points, their cryptographic function cannot easily be changed by the user and they are designed for installation by
the user without further substantial support by the supplier. These are exempted by the ‘Cryptography Note’ in the dual-use control list: the interpretation of this is notoriously difficult and is discussed further in the next section;

6) components or software designed to be incorporated into existing items exempted by the Cryptography Note. To qualify, such products must not have information security as their primary function or set of functions, they must not change or add any cryptographic functionality to the existing items, and their feature set must not be designed or modified to customer specifications;

7) items if their primary function or set of functions are not: information security; a computer (including operating systems and components); sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or networking.

How are these exemptions applied?

While the majority of these exemptions are relatively straightforward, there are significant differences between regulators in their interpretation of the Cryptography Note. In the UK, the exemption is, in practice, permitted only to low price, high-volume products purchased from high street stores or online, for retail/home users. Precisely how these are defined remains a matter of subjective judgement.

This is causing serious difficulties, in addition to the administrative burden of licensing ever-larger volumes of goods. An exporter may assess that a new product does not require a licence but finds that it is held at the border while the customs authorities confirm whether a licence is required. At best this causes minor delays but, if the UK’s Export Control Organisation (ECO) decides that a licence is required, there can be a substantial delay while a licence is obtained, and the exporter risks facing enforcement action for breaching export control regulations. There is a particular risk of this when UK companies are exporting items that have already been classified in the US as ‘mass market’ and do not require a US export licence. Since the UK interprets the rules differently, such items may nonetheless require a licence in the UK.

As a result, some UK companies are routing business to overseas branches in countries where the rules are interpreted less restrictively. It is conservatively estimated that this is causing a loss of exports from the UK worth over £50 million per annum. In response, it is understood that the ECO is pursuing a number of initiatives:

1) the adoption of an approach closer to that of the US. But ECO officials have made clear that they have no intention of adopting the US concept of ‘mass market’ and will continue to confine the exemption to products intended primarily for retail to consumers and not to those intended for commercial use;

2) with respect to components, the ECO is already satisfied with being given examples of the types of product into which the component will be incorporated, without needing to know all its possible uses. In future, if a component is specifically designed for an exempted consumer-type product, then a statement of design intent may be sufficient to allow exemption. The ECO also intends to consider whether to exempt components designed for consumer-type products that are still under development;

3) the development of new, expanded guidance to help exporters judge for themselves whether their products qualify for exemption;

4) the restart of its former goods classification advice service, possibly later this year, as soon as trained staff are available. This will enable exporters to ask the ECO for a determination of whether a specific item is subject to control, without having to apply for a licence. The ECO is to consider including in its responses generic advice on how a ‘No Licence Required’ ruling was determined to help exporters understand the rationale for the control rating, in order to be able to conduct their own classifications;
working with other Governments in the Wassenaar Arrangement (the international export control regime that establishes the list of dual-use items used by the EU, the US and most others) to revise the controls on information security items in the Regulation. Their aim is completely to restructure and rewrite the text, to produce a positive list of items subject to controls in place of the current approach involving a catch-all combined with a range of exemptions. It is hoped that a revised text for this section of the Regulation will be agreed by the end of 2016 and brought into effect next year;

the development of an Open General Export Licence for cryptographic items that are not eligible for exemption but are nonetheless relatively low risk. The challenge is to strike a balance between the range of items included on the one hand, and the range of end-users and destinations on the other. The ECO has invited suggestions from exporters of classes and types of products which could be considered for inclusion, focused on items that currently generate a high volume of standard individual export licence applications. Initial ideas include: prototype commercial mobile phones and components using published standards (e.g. ETSI, GSM, 3GPP); Unified Threat Management devices and software designed for commercial uses; routers, servers and network hardware for commercial use; development boards and integrated circuits that employ encryption where encryption is not the primary function; satellite communication equipment meeting International standards; open source software using published standards; business transaction management software; commercial secure access service software including network key devices for PCs, laptops and tablets; and technology relating to these goods. Industry want government agencies and government-controlled organizations included as permitted end-users, and all destinations covered except for countries subject to EU sanctions (i.e. Russia would be excluded but China would be included). But the details remain to be worked out by the industry and negotiated with the ECO.

What else may be changing?

The European Commission is expected to publish its proposed revision to the Regulation soon. In its public information on the proposals, the Commission stated that it was considering a number of issues relevant to controls on encryption, in particular:

- possible new controls on cyber surveillance items, including an EU list of such items and end-use controls to require licensing of any item that might be used for cyber surveillance;

- an EU General Export Authorisation for cryptographic items (which seems likely to overlap significantly with the ECO’s new OGEL outlined above);

- a requirement to apply human rights criteria not only to military items (as now) but also to dual-use items. This would not make a significant difference in the UK which already applies human rights criteria to all dual-use export licence applications.

The UK’s intended exit from the EU also raises a number of questions over the future shape of the UK’s export licensing and sanctions regimes, in particular what licensing will be required for trade in dual-use goods between the UK and the remaining EU countries, whether UK and EU control lists and licensing policies will diverge and what will be the impact on UK dual-use trade with countries outside the EU. Broader issues raised by Brexit for UK technology companies include any restrictions on free access to the EU internal market, how far the UK remains subject to EU regulations and the related risk of non-tariff barriers (such as different labelling or supply chain standards); the ability to recruit and retain skilled staff, government funding of research, the UK’s new trading relationships with third countries, protecting intellectual property and ensuring the free flow of data.

What does this mean for companies and how can Dechert help?

Breaches of export controls are a criminal offence and can result in the seizure of goods, an unlimited compound penalty and/or prison. Companies that export cryptographic items need to ensure that their compliance
procedures are fully effective in determining whether their items require a licence and if so which licence is most suitable, and in fulfilling the conditions of their licences. They should exercise particular caution in applying any of the exemptions, especially in the case of US-origin items that are classified as 'mass market' in the US since these may nonetheless require a licence in the UK. They should consider contributing suggestions for items, end-users and destinations they want to see included in the proposed new Open General Export Licence. They should also consider the potential impact on their business of the revised EU Regulation and of Brexit, and engaging with the ECO to ensure that their interests and concerns are taken into account.

Members of Dechert’s International Trade and EU Law Team have extensive experience, including as former regulators, in helping companies to understand and to implement export control, sanctions and other trade-related regulations applicable to their business, across a range of jurisdiction including the US.

Dechert’s team are also ideally placed to help companies to analyze the potential opportunities and risks of Brexit for their business, and to engage with the UK and EU governments and institutions to promote and to defend their interests. In the light of the uncertainties created by both Brexit and the developments outlined above, companies exporting these types of products may wish to consider undertaking a quick review of their export controls matrix to identify potential risks and vulnerabilities going forward.

For further information, please contact:

Miriam Gonzalez
Partner, London
T: +44 20 7184 7892
miriam.gonzalez@dechert.com

Richard Tauwhare
Senior Director, London
T: +44 20 7184 7350
richard.tauwhare@dechert.com

© 2016 Dechert LLP. All rights reserved. This publication should not be considered as legal opinions on specific facts or as a substitute for legal counsel. It is provided by Dechert LLP as a general informational service and may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome. We can be reached at the following postal addresses: in the US: 1095 Avenue of the Americas, New York, NY 10036-6797 (+1 212 698 3500); in Hong Kong: 27/F Henley Building, 5 Queen's Road Central, Hong Kong (+852 3518 4700); and in the UK: 160 Queen Victoria Street, London EC4V 4QQ (+44 20 7184 7000).

Dechert internationally is a combination of separate limited liability partnerships and other entities registered in different jurisdictions. Dechert has more than 900 qualified lawyers and 700 staff members in its offices in Belgium, China, France, Germany, Georgia, Hong Kong, Ireland, Kazakhstan, Luxembourg, Russia, Singapore, the United Arab Emirates, the UK and the US. Further details of these partnership and entities can be found at dechert.com on our Legal Notices page.
Thank You

For further information, visit our website at dechert.com

Dechert practices as a limited liability partnership or limited liability company other than in Dublin and Hong Kong.