

OVERSEAS STORAGE OF ELECTRONIC INFORMATION

INTRODUCTION

1. This paper is produced by the Export Group for Aerospace and Defence (EGAD) in an attempt to clarify the issues and concerns surrounding the overseas storage and management of electronic information. It is intended only as a guide to the principles involved, and is not intended to be authoritative. If affected by these issues, companies should seek their own legal advice.

SCOPE

2. Increasing globalisation and an increasing need to drive down costs mean that more and more companies wish to store or manage information electronically outside the country in which that information is generated or used. Companies frequently need to have computer servers in one country accessed by users¹ in another, or servers in one country managed by administrators² in another. In either case, the company's IT support may be outsourced to a third party provider, and that provider may be subject to another Nation's legislation.

LEGISLATION

3. Key legislation covering the issues is contained in:

- 3.1. UK Data Protection Act 1998, associated with the EU Data Protection Directive (95/46/EC 1995)
- 3.2. UK Export Control Act 2002, and its subsidiary secondary legislation (The Export of Goods, Transfer of Technology and Provision of Technical Assistance (Control) Order 2003 (SI 2003 No 2764))
- 3.3. EU Council Regulation (EC) No 1334/2000 as amended
- 3.4. US International Traffic in Arms Regulations (22CFR §120 – 130) (Issued under the terms of the Arms Export Control Act (22 USC 2778))
- 3.5. US Export Administration Regulations Parts 730-774 (Issued under the terms of the International Emergency Economic Powers Act, as amended)

WHAT INFORMATION IS OF CONCERN?

4. Broadly speaking, there are 3 groups of information that should be of concern to organisations seeking to store or access electronic information overseas: personal data, information or technology controlled under national and international "military" regulations, and information or technology controlled under national and international "dual use" regulations.

¹ "User" – person authorised by the computer manager to run programmes on a computer, usually with pre-defined limitations on levels of access.

² "Administrator" – person who has access to all aspects of a computer, and is able to set permissions for other users. An administrator will normally be able to see all data on a computer and operate all programmes.

5. Personal Data.

5.1. Personal data includes names, addresses, pay, banking and other personal details. It may also include computer log-in IDs where these can be linked back to an individual.

5.2. The UK Data Protection Act (and most EU Privacy laws) define 2 roles in the protection of personal data:

5.2.1. Data Controller, which is the entity that defines the purposes for which and the manner in which the personal data will be used (the 'owner' of the data).

5.2.2. Data Processor, the entity that processes the data on behalf of the Data Controller.

5.3. Where an IT provider holds or processes personal data on behalf of a client, then the client has the role of Data Controller and the service provider has the role of Data Processor. The Data Controller is held liable for compliance with the law and has the responsibility of ensuring that any contractor (Data Processor) they use applies appropriate safeguards to maintain that compliance.

5.4. If the transfer of personal data is limited to within the EEA³ then there is no reason in terms of privacy and data protection law for the client to object, as all the EU country privacy and data protection laws allow such transfers. (One of the aims of the EU Data Protection Directive is to enable the free flow of personal data across the EU.) If the transfer is from the EU to a non-EU country with a privacy law that has been approved ('finding of adequacy')⁴ by the European Commission it will also be allowed under data protection laws.

5.5. If the transfer is from the EU to a non-EU country which does not have a 'finding of adequacy' by the European Commission then there are particular legal requirements that Data Controllers have to adhere to. A common way for Data Controllers to meet these legal obligations is to require the Data Processor (service provider) to sign an EU Standard Contract for Data Controller to Data Processor transfers. Some EU countries require the prior approval of EU Standard Contracts by its regulator **before** the transfers may be made out of that country.

5.6. No "finding of adequacy" has been made in respect of the USA as the USA has no Federal privacy law deemed acceptable by the EU. Some US companies sign up to a "Safe Harbor" code of practice on the protection of personal data which is a voluntary bi-lateral agreement between the EU and the USA that meets the requirements of the EU Directive.

6. Military Information

6.1. "Military information" stored electronically can include software, military technical data, and "technology" – which comprises specific information required for the development, production or use of controlled goods or software. It is controlled under local National legislation, and will normally require an export licence before it can be moved, or accessed, across National borders.

6.2. If the information is of US origin and has been exported to a destination in the UK, it will also be controlled by the US International Traffic in Arms Regulations (ITAR), and will require a US export license (in addition to any necessary UK licence) before it can be transferred to a third party in the UK, re-

³ The EEA consists of the 25 EU member countries plus Norway, Iceland and Lichtenstein.

⁴ As at June 2007 the following countries have a 'finding of adequacy': Argentina, Canada, Guernsey, Isle of Man and Switzerland

exported from the UK to a third country, or accessed by a national of a third country (whether in the UK or not). These additional ITAR constraints in particular make it imperative that companies holding nationally military-controlled data or ITAR-controlled data consider the implications carefully before employing an external IT provider, using an overseas based IT helpdesk, or storing their information offshore.

7. Dual-Use Information

7.1. Information categorised as “Dual Use” (detailed in Article 3 of Council Regulation (EC) No 1334/2000 as amended) can again include software, technical data, and “technology” – which comprises specific information required for the development, production or use of controlled goods or software. However, dual-use software which meets the requirements of the General Software Note⁵ is exempted from the EU controls, as is software containing cryptography which meets the requirements of the Cryptographic Note⁶. Material in this list may be exported freely between the member states of the EU, but would need an export licence to be exported from the EU (unless it is to be hand-carried by an individual for his/her personal use).

7.2. If the material is of US origin, it may, in addition, be controlled by the US Export Administration Regulations (EAR). The US list contained in the EAR is broader than the EU list, and imposes some additional constraints. In particular, the US treatment of cryptographic material – including that contained in commercially-available US-manufactured software such as Windows – is different. Specialist advice is required, particularly if such software is to be exported to a destination outside the EU. Also, while Space-related goods are controlled by Category 9 of the EU Dual-Use list, the US State Dept treats them as military goods and exercises jurisdiction over them through the ITAR (not the EAR)

SERVER LOCATION

8. The brief summary of the applicable legislation given above leads to several possible scenarios that companies should consider when storing information electronically, whether it be on an e-mail server, ftp server, company intranet site or on an electronic database:

9. Server Outside the UK, But Not In the US

9.1. The DTI Guidance Note⁷ on the UK legislation says – at Q10 – that *“Whether or not a licence is required depends on where the recipient of an electronic transfer is located, not on where the technology or software may be routed in the course of its transfer. Thus, electronic transfers of military (or dual use) technology to recipients in the UK would not be subject to control simply because the transfers were or might be routed via a server located abroad (assuming the server was not accessible outside the UK by normal means). It is the geographical location of the recipient which dictates whether or not a licence is required. Similarly, technology or software on files saved to a server overseas, or on files sent electronically to overseas file storage, would not be subject to*

⁵ Known as the “Dixon’s Test” – briefly: available from stock for retail sale and designed for installation by the user without further substantial support by the supplier

⁶ Similar to the General Software Note, but containing additional constraints. Detailed in the DTI guidance at <http://www.dti.gov.uk/europeandtrade/strategic-export-control/licensing-rating/guidance/page8489.html>

⁷ <http://www.dti.gov.uk/files/file7981.pdf>

control, unless the information in question was to be made accessible from outside the UK in the process.

9.2. No attempt is made in the Regulations to control intermediate servers handling material in course of transfer – so Internet Service Providers may have servers located overseas; it's the end point of the transfer that matters ("server not accessible outside the UK by normal means"). However, files stored electronically overseas (on an overseas server) would be subject to control if the information in question was to be made accessible by normal means from outside the UK in the process.

9.3. However, anyone with "Administrator" rights to a server would "normally" have access to all the programmes and data held on that server, and so the "Administrator" would need an export licence if outside the UK. If the data is encrypted on the server, then it could be argued that only someone with access to the decrypt key would "normally" have access to the data.⁸

10. Server In The US:

10.1. If information is held (electronically or otherwise) in the US, it becomes subject to US export controls, regardless of its origin.

10.2. The ITAR (22CFR) §120.6 defines "Defense Article" as including technical data, while §120.17 defines "export" as "sending or taking a defense article out of the United States by any manner..." There appears to be no relaxation of this rule even if the data is held in the US in encrypted form and not accessible by anyone in the US.

10.3. Current US opinion is thus that if controlled information is held on a computer which is physically in the US, an export authority of some sort (license, exception, exemption⁹ or Technical Assistance Agreement) would be required before the information could be accessed from outside the US, or by a "foreign" (ie non-US) person in the US. That requirement applies whether or not the information is encrypted, and whether or not the information is of US origin.

10.4. A UK company storing its own data on a server in the US is therefore potentially making that data subject to US controls. (In theory, this applies equally whether or not the company has any control over where the data is stored – for example in a web vault or back-up repository provided by a third party)

10.5. Similarly, a US company would be ill-advised to hold US-controlled data on a server outside the USA, whether or not that data is encrypted.

11. Third Party IT Providers.

11.1. The responsibility for ensuring that data is controlled in accordance with all applicable legislation remains with the company providing the data, and any constraints on that data should be imposed on anyone handling that data. Companies which employ a third-party IT provider therefore need to tell that provider if information is subject to local national or US export controls, to allow the IT provider to protect the information appropriately. (For example, if data is controlled by ITAR, companies will need to ensure that the appropriate US export license (usually a TAA) is in place to allow the IT provider to access the data, and the IT provider may need to impose nationality constraints on who may

⁸ This does not appear to have been tested in court.

⁹ ITAR §125.4(b)(7) provides an exemption for technical data being returned to its original source of import.

access the material; don't forget that computer administrators can normally access any material on the computer).

11.2. Companies using external IT providers should ensure the contract with the IT provider requires that IT provider to seek the Company's written permission before holding information on offshore servers, accessing such information from offshore, or (if applicable) allowing access to information in the UK to non-UK persons, including dual nationals.

11.3. Even if there is no mention of the subject in the contract, IT providers should check with customer Companies before any server, or its support, is moved to an offshore location. (Not all companies are aware of the implications of local national export control legislation on their products) They should check:

11.3.1. Whether any of the customer's data is controlled by US or local national export legislation, and if so, what controls apply to it

11.3.2. Whether any of the customer's data may be controlled by UK/EU data privacy legislation, and if so, whether the proposed offshore location provides sufficient data protection

11.3.3. Whether any of the applications hosted on the computer(s) in question are controlled by US or local national export legislation (for example: whether the application employs controlled cryptography, especially if the software is of US origin, or whether any of the software is itself controlled by the national Military or Dual Use List)

12. Help Desks/Remote Administrators

12.1. In the same way that computer administrators will normally be able to access all material on a computer, individuals operating a corporate help desk will often have the ability to view (and sometimes take control of) a company employee's computer screen, and have access to any information that may be displayed. If this is possible, and the displayed information is controlled in any way, then it may be necessary for help desk staff to be licensed to view it (particularly if the help desk is overseas).

13. Overseas Software Developers

13.1. Care should also be taken to ensure that access to systems by overseas software developers does not breach export legislation – for example by giving them access to live data or controlled software.

SUMMARY

14. Export and data protection controls affect three main groups of information (personal data, military information and dual-use information). Companies storing that information electronically should consider the legal implications of holding that data on computer servers overseas (particularly in the USA). The use of third party IT providers, overseas help desks, remote computer administration and overseas software developers all provide potential ways of breaching export control legislation.

David Wilson

EGAD EC

7th June 2007