DWP Department for Work and Pensions

March/April 2008

Dear Supplier,

SECURITY OF DATA HANDLING PROCEDURES

I am writing to seek your assurance about your handling of the Department's information that relates to individual people – i.e. personal data, about which I have provided further information below.

You may be aware that last November, following the loss of CDs in HM Revenue and Customs, the Prime Minister announced that the Cabinet Office would undertake a review into the way that government departments use and store personal data.

Recently a laptop computer was stolen from the parked vehicle of a naval officer, and that laptop contained the personal details including passport, bank account and National Insurance numbers of 600,000 individuals. The data on the laptop was not encrypted or otherwise protected in any way.

In the wake of that latter incident, the Cabinet Office has now instructed all departments in the following terms, and instructed us to pass this message on to all our delivery partners:

From now on, no unencrypted laptops or drives containing personal data should be taken out of secured office premises. Please ensure that this is communicated throughout your organisation and delivery bodies and implemented immediately, and that steps are taken to ensure compliance.

This instruction is being applied by the Department to all our laptop computers, and also includes those removable portable devices or media which can store personal data, and be connected to a computer, such as flash drives, memory sticks and pens, thumb drives, and removable hard drives, as well as CDs and DVDs, etc. It will also include devices such as PDAs or Blackberry phones where they have been used to store or process personal data. We are ensuring that laptops and such devices are encrypted. In this case, 'encryption' means full disk encryption. Where a laptop is not encrypted, then it must not be taken out of the office if it contains personal data.

In terms of 'personal data', the Information Commissioner does provide advice on his website, however in simple terms, we have taken this term to include any personal information about a customer of the Department (or for that matter an employee or contractor), the compromise, loss or theft of which could cause distress or harm to that individual. Thus the obvious details which need to be protected include:

Names, together with any other information which could identify that person, such as:

Address;

Date of birth;
NI Number;
Telephone numbers;
Benefit details;
Bank account details;
Information relating to the person's health or disability;
Employment history.

In a further recent case, where the Commissioner has taken enforcement action, he has advised organisations that they must have adequate security procedures in place to protect personal information for example password protection **and** encryption.

You may already be taking steps to protect your organisation's data in the light of recent incidents. However, the Department needs to be assured that, if you have not already done so, you will take immediate action to ensure that any personal data which you are processing on behalf of the Department and is taken out of your premises:

- on laptop computers; or
- on any removable devices or media,

will be protected by encryption ideally to at least the FIPS 140-2 standard.

This encryption requirement applies to Departmental information on laptops/removable media handled by both your employees and sub-contractors.

We understand that if not already done so, you will need to obtain suitable encryption software. The Information Commissioner's website provides helpful advice at: http://www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx, and also has a link to the Government-sponsored 'Get Safe Online' website.

Although these pages provide guidance on the standards to be followed, you will probably have to take professional advice to ensure product compatibility with your own systems.

Whilst the Cabinet Office's instruction refers to laptops and other removable media, you should also review your procedures for handling paper documents to ensure that they are safely stored, handled and transported in a way that is commensurate with those standards that now apply to electronic media. Data, which is no longer required by you for processing on the Department's behalf, must be returned.

Equally, although this instruction relates specifically to personal data, we expect that you will make arrangements to review and safeguard any other information that you are processing on behalf of the Department.

If there are any incidents where the Department's personal data is stolen from you or your contractors, or is mislaid or lost, you must advise the Department's nominated contract manager immediately by telephone and then promptly confirmed in writing.

Would you please reply to this letter within seven days to confirm that you have implemented these new rules in relation to any personal data that you have received, or will receive in future, from the Department.

To assist you in doing so I attach a copy of this letter which is annotated to provide for it to be signed on behalf of your organisation thereby providing confirmation that the obligations set out in the letter are accepted. It should be returned to me at the above address by 18 March 2008.

If you require any further information, would you please contact your Departmental contract manager in the first instance.

Yours sincerely,

David Smith
Commercial Director

.....