

John Sharpe
Information Strategy Team
Room 4/52
100 Parliament Street
London SW1A 2BQ

Frank [request-21466-3xxxxxx@xxxxxxxxxxxxxxx.xxx]

by e-mail

Tel

Fax 020 7147 0666

Email

www.hmrc.gov.uk

Date 18 November 2009

Our Ref FOI 2316/09

Your Ref

Dear Mr Mustill

You asked in relation to HMRC:

Please could you tell me how many breaches of the Data Protection Act have happened and been logged within the last 5 years?

What was the data that was subject to the breaches (brief description will suffice as I realise you may not be able to go into detail)?

Have there been investigations by the Information Commissioner's Office in relation to the breaches of the Data Protection Act and what were the findings of the investigations?

Have there been any fines or penalties imposed on the HMRC in relation to these breaches?

Has the HMRC signed any type of formal undertaking to guarantee compliance with the Data Protection Act?

Has the HMRC signed any type of formal undertaking to guarantee compliance with the Data Protection Act?

Has there been any reviews of the inadequate risk assessment and security procedures that were in place at the time of these breaches?

Information is available in large print, audio tape and Braille formats.
Type Talk service prefix number – 18001



INVESTOR IN PEOPLE



Has there been any reviews on due diligence procedures in relation to data management and protection?

Has there been any reviews of data protection policy and have any new systems of administration and monitoring been established to combat breaches in the Data Protection Act?

HMRC does hold information falling in the scope of your request but we estimate that the cost of complying with it would exceed the appropriate limit of £600. This is because the information is contained in records that pre-date the creation of this department in 2005 and to obtain the information would mean that the appropriate limit as specified in regulations would be breached. Currently, and for central government, the limit is set at £600. This represents the estimated cost of one person spending 3½ working days determining if the department holds the information. This includes locating, retrieving and extracting the information. Under section 12(1) of the Freedom of Information Act 2000 the department is not obliged to comply with your request and we will not be processing it further.

If you have any queries about this letter, please contact me. Please remember to quote the reference number above in any future communications.

If you are not happy with this reply you may request a review by writing to HMRC FOI Team, Room 4/52, 100 Parliament Street London SW1A 2BQ. You must request a review within 2 months of the date of this letter. It would assist our review if you set out which aspects of the reply concern you and why you are dissatisfied.

If you are not content with the outcome of an internal review, you may apply directly to the Information Commissioner for a decision. The Information Commissioner will not usually consider a case unless you have exhausted the internal review procedure provided by HMRC. He can be contacted at The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Because part of your request exceeds the limit HMRC is not required to answer any part of it but there is some readily available information which I can supply; I am doing that outside the strict terms of Act.

The information I can provide is that following the well publicised loss in 2007 of 2 CDs containing personal information on up to 25 million individuals the Information Commissioner (ICO) considered the report into the review of information security by Kieran Poynter. You will find the report on the Treasury website here:
http://www.hm-treasury.gov.uk/poynter_review_index.htm .

The Commissioner served an enforcement notice on HMRC in July 2008 stating that HMRC should use its best endeavours to implement all 45 recommendations made by Kieran Poynter by 31 July 2011. You will find the notice on the ICO website at this link:
http://www.ico.gov.uk/upload/documents/library/data_protection/notices/hmrc_en_final.pdf

HMRC continues to work to implement all of the recommendations in the review and comply with the ICO enforcement notice.

HMRC has not signed any formal agreement to comply with the Data Protection Act; there would be no need as the act binds all data controllers and provides sanctions for those that do not comply. Other than the notice mentioned above there have been no penalties or sanctions imposed on HMRC for breaches of the Data Protection Act.

In order to assist with any reformulated request you may find it helpful if I tell you that the most expensive parts of your request in compliance terms are:-

- Items 1 and 2 because we do not hold figures for before the creation of HMRC in April 2005 for later years we do not record in detail whether some misuse of our computer systems might constitute a breach of the Data Protection Act.
- Collating all the internal changes in Data Protection policy and practice although they do mirror the requirement identified in the Pontyer report.

Yours sincerely

John Sharpe