



The Association of Independent Financial Advisers

Response to the Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998

AIFA is the trade association that represents UK regulated independent financial advisers (IFAs). Membership of AIFA is voluntary and on a corporate basis. AIFA currently represents over 80% of IFA firms in the UK.

IFA firms are the leading distribution channel for retail financial products in the UK. Last year they generated 73% of business by monetary value and are the major sector advising and arranging retail life and investment products in the UK. As such, IFAs represent a dominant force in the maintenance of a competitive and dynamic retail financial services market.

The protection of personal information is important to us all both as firms that handle consumers' information and as consumers.

Question 1 – Do you agree that data controllers should have the opportunity to provide consent for a Good Practice Assessment (GPA) when registering with the Information Commissioner's Office?

We agree that data controllers should be able to consent to a GPA but this should not be made mandatory.

Our members are all regulated by the Financial Services Authority (FSA) and therefore already come under scrutiny for the security of their clients' data. Data security is high on the FSA's agenda and they conduct monitoring visits in this area. Where an area is covered by two regulators we would wish to see a lead regulator take responsibility for any action that is deemed necessary for a breach that falls within both regulators remit, rather than have firms facing double jeopardy on the same issue. Dual regulation is not good regulation.

Question 2 – Do you agree with the proposed three-month notice period for data controllers to withdraw consent for a GPA?

It seems reasonable that a notice period for withdrawal of consent is applied.

Question 3 – Do you agree with the proposal to exempt data controllers who consent to a GPA from the civil monetary penalty under section 55A of the Data Protection Act 1998 (once in force) for a breach discovered in the process of a GPA?

Exempting data controllers from a monetary penalty when a breach is unforeseen or unintended is acceptable. But putting in place an exemption for data controllers who have given prior consent to a GPA, but are knowingly and deliberately in breach, seems to be a surprising position to take. Caution should be exercised before giving inducements to controllers that disregard the rules.

Question 4 – Do you agree that when the Commissioner issues an information Notice under section 43 of the DPA 1998 he should have the power to specify the time and place that information should be provided to him?

We agree that a deadline has to be put on to the provision of information with the understanding that this should be applied reasonably. There will be circumstances that demand immediate action in order to prevent detriment to consumers and in such cases the ICO needs to move swiftly. For more routine information we would expect due consideration to be given to allow time for production of information or visit to be arranged.

Question 5 – Do you agree that the information Commissioner should be able to enter a data controllers' premises under a court warrant to undertake an inspection in circumstances where:

a) He does not have reason to suspect non-compliance or a breach of the data protection principles?

Obtaining a court warrant if there is no reason to suspect non-compliance or a breach appears both extreme and disproportionate. If after exhausting its other powers, ICO considers it necessary to apply for a warrant one would expect that suspicion is present and the data controller is not co-operating or is withholding information.

b) He does not have reason to suspect non-compliance or a breach of the data Protection principles but has completed a risk-assessment which identifies the data controller as high-risk?

Although a data controller may be considered high risk, this does not automatically mean he/she is in breach. Again caution must be exercised and the application for a court warrant should be considered as last resort.

Question 6 – Do you agree that the Information Commissioner should have the power to require any person on the premises, where a warrant is being

executed, to provide the Commissioner with any information required to determine whether the data controller has complied with or is complying with the data protection principles?

When a warrant is being executed it is reasonable to require the relevant people on the premises to provide any information relevant to the ICO's investigation. In small firms this is likely to be all or most of the staff but in larger firms there will be many employees who do not have any dealings or knowledge of the data controllers scope of work. It would be unreasonable to expect such people to be able to assist in an enquiry.

Question 7 – Do you agree with the proposal to introduce a tiered notification fee structure to ensure the extent of regulatory activity required by the ICO is reflected more accurately in the level of notification?

It would seem fair to introduce a tiered fee structure to ensure the extent of regulatory activity required by the ICO is commensurate with the cost but without more information we are unable to comment in more detail.

Question 8 – Do you consider it proportionate and appropriate that there should be an additional penalty, other than removal from the register, for data controllers who knowingly and deliberately provide incorrect information as part of their notification fee assessment?

We would like to see a pragmatic approach applied when considering any additional penalty when incorrect information has been provided.