DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

DATED: 5 January 2016

To: Alzheimer's Society

of: Devon House
58 St Katharine's Way
London E1W 1LB

1. Alzheimer's Society is the data controller, as defined in section 1(1) of the Data Protection Act 1998 (the 'DPA'), in respect of the processing of personal data by the Alzheimer's Society and is referred to in this notice as the data controller.

2. The Commissioner issued the data controller with an Undertaking in February 2010 to ensure that remedial action was taken following a security breach that was investigated by the ICO.

3. The ICO also carried out an audit of the data controller in March 2013 which provided 'reasonable assurance'. The ICO then carried out a 'follow-up' audit in March 2014 which revealed that a recommendation in the ICO's March 2013 audit report had not been fully implemented by the data controller.

4. The ICO has now carried out a further investigation into the data controller's compliance with the provisions of the DPA following a second security breach that was discovered on 15 April 2015.

5. The Commissioner has considered the data controller's compliance with the provisions of the DPA in light of these

matters.

6. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, it is the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller. The relevant provisions of the DPA are the Fifth and Seventh Data Protection Principles.

7. The Fifth Data Protection Principle provides at Part I of Schedule 1 to the DPA that:

> *"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".*

8. The Seventh Data Protection Principle provides at Part I of Schedule 1 to the DPA that:

> *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".*

Paragraph 9 of Part II of Schedule 1 to the DPA further provides that:

> *"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to –*
>
> *(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and*
> *(b) the nature of the data to be protected."*

9. Having considered the facts of this case, the Commissioner is satisfied that the data controller has contravened the Fifth Data

Protection Principle in that the data controller has kept personal data for longer than is necessary for the purpose of the processing.

10. The Commissioner is also satisfied that the data controller has contravened the Seventh Data Protection Principle in that the data controller failed to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

11. The Commissioner considered, as he is required to do under section 40(2) of the DPA when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner took the view that the likelihood of distress to the data controller's data subjects is self-evident.

In view of the matters referred to above the Commissioner hereby gives notice that, in exercise of his powers under section 40 of the Act, he requires that the Alzheimer's Society shall within 6 months of the date of this Notice take steps to ensure that:

(1) Personal data is not kept for longer than is necessary;

(2) There is a mandatory data protection training programme for all staff (including volunteers who have access to personal data) and refresher training at least every two years. Delivery of the training should be tailored to reflect the needs of both staff and volunteers;

(3) Completion of any such training is monitored and properly documented;

(4) Policies and procedures relating to data protection and information governance are brought to the attention of all staff (including volunteers who have access to personal data);

(5) Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are all encrypted using encryption software which meets the current standard or equivalent;

(6) Secure email accounts are provided to all staff (including volunteers who process personal data by email in connection with their work for the data controller);

(7) Secure storage is provided for all staff (including volunteers who hold hard copy records containing personal data in connection with their work for the data controller);

(8) Manual (as well as automated) checks are made to identify vulnerabilities on the data controller's website e.g. penetration testing;

(9) Appropriate organisational and technical measures are taken against the unauthorised access by staff (including volunteers) to personal data;

(10) Paragraphs 11 and 12 of Part II of Schedule 1 to the DPA are complied with where processing of personal data is carried out by a data processor on behalf of the data controller.

There is a right of appeal against this Notice to the First-tier Tribunal (Information Rights), part of the General Regulatory Chamber. Information about appeals is set out in the attached Annex 1.

Dated the 5th day of January 2016

Signed: ……..
Stephen Eckersley
Head of Enforcement
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom an enforcement notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Leicester
   LE1 8DJ

   Tel: 0300 1234504
   Fax: 0870 739 5836
   Email: GRC@hmcts.gsi.gov.uk
   Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

   The notice of appeal should be served on the Tribunal within 28 days of the date on which the enforcement notice was sent.

4. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998,

and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).