Personal Data Breach

Throughout this policy we may make reference to Age Concern Liverpool & Sefton, the Organisation or ACL&S. This means however that the policy is applicable to the Charity, Age Concern Liverpool & Sefton, the trading company, Age Concern Liverpool (Services) Ltd and any subsequent company within the group

1. Scope

This procedure applies in the following events:

1. A personal data breach pursuant to Article 33 '*Notification of a personal data breach to the supervisory authority',* and

2. A personal data breach pursuant to Article 34 *'Communication of a personal data breach to the data subject'* of the GDPR.

2. Data controller and data processor

There is a distinction under the GDPR between a 'data controller' and a 'data processor'. This is because different organisations involved in processing personal data have varying degrees of responsibility. An organisation must choose whether it is a data controller or a data processor as regards a particular activity and cannot be both.

3. Responsibility

All users, including temporary employees of Age Concern Liverpool & Sefton and third parties, and Age Concern Liverpool & Sefton must be aware of this procedure and are required to follow it should a personal data breach incident occur.

4. Procedure – Breach Notification

Data processor to data controller

All personal data breaches by Age Concern Liverpool & Sefton must be notified to the appropriate data controller immediately. The Chief Executive (CEO)/Chief Operating Officer (COO) must record the communication of the breach in the Internal Personal Data Breach Register, stating how the notification was made (whether my email, telephone call etc.), to whom and how the confirmation of receipt was provided.

Data controller to supervisory authority

All personal data breaches by Age Concern Liverpool & Sefton must be notified to the appropriate supervisory authority immediately.

Age Concern Liverpool & Sefton is required to carry out an assessment in order to determine whether the personal data breach is likely cause a risk to the affected data subject's rights and freedoms under the GDPR.

If a risk is considered likely, Age Concern Liverpool & Sefton is required to report the personal data breach to the supervisory authority immediately and in any event, no later than 72 hours after the risk assessment. If the notification is made outside of the 72 hour window, Age Concern Liverpool & Sefton is required to provide reasons for the delay.

Pursuant to the External Breach Notification Record, Age Concern Liverpool & Sefton is required to provide the following to the supervisory authority:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Age Concern Liverpool & Sefton to address and/or mitigate the breach; and
- All other information regarding the data breach.

The CEO/COO must record the communication of the breach in the Internal Personal Data Breach Register, stating how the notification was made (whether my email, telephone call etc.), to whom and how the confirmation of receipt was provided.

Data controller to data subject

If it is likely that there will be a high risk to the affected data subject's rights and freedoms under the GDPR, Age Concern Liverpool & Sefton is required to provide immediate notification to the relevant data subjects.

The notification to the data subject must be made in clear and plain language and must include the following:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Age Concern Liverpool & Sefton to address and/or mitigate the breach; and
- All other information regarding the data breach.

Age Concern Liverpool & Sefton must use appropriate measures, such as encryption or password protection, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority.

Age Concern Liverpool & Sefton must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue.

If notification would require Age Concern Liverpool & Sefton to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, so long as all data subject are effectively informed.

It is possible that the supervisory authority may require Age Concern Liverpool & Sefton to communicate the personal data breach to the data subject, should there be an element of high risk involved.

5. Document owner

The Chief Executive (CEO)/Chief Operating Officer (COO) is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 5 February 2020 is available to all employees of Age Concern Liverpool & Sefton on the corporate intranet.

This policy document was approved by Age Concern Liverpool & Sefton's Policy Scrutiny Committee which is composed of Trustees and is issued by the CEO/COO on a version controlled basis.

CEO/COO
Date: February 2020
Review Date: February 2021
V2