Data Breach policy

In compliance with European data protection laws, CARE International UK (CIUK) may be required to notify its regulators of any actual or suspected breach of security leading to any of the following events:

- the accidental or unauthorised loss of, destruction of, or loss of access to, personal data
- the alteration of, or unauthorised disclosure of or access to, personal data; or
- other misuse involving personal data (together a "**Data Breach**").

Data Breaches are not limited to malicious actions such as hacking of systems, virus infection or theft of electronic data. In practice, Data Breaches will more frequently arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure. For example, where portable devices, such as laptops or smartphones which store business-related personal data are lost, stolen or not disposed of appropriately, or where emails are inadvertently sent to an incorrect recipient.

CIUK has a legal obligation to notify the ICO within 72 hours of becoming aware of certain Data Breaches. Not all Data Breaches need to be notified to the regulator if you do not have the appropriate authority you must not contact the regulator directly.

If you become aware of a Data Breach, you must immediately report it to the Data Protection Working Group. This will enable the correct people to assess whether CIUK needs to notify the regulator of the Data Breach.

CIUK may need to notify multiple regulators. It is therefore critical that its response to a Data Breach is coordinated and that the message to all regulators is aligned.

1. Preventing and detecting Data Breaches

Prevention and detection of Data Breaches is a responsibility for everyone at CIUK. Each staff member should be aware of his/her duties in this context.

You must therefore apply caution and common sense when using CIUK's IT infrastructure and handling CIUK's data, in particular personal data. You should read and comply with CIUK's IT Security and Data Protection Policies which give you detailed guidance on how to act responsibly and protect CIUK's business.

When it comes to detection of Data Breaches, you are a key element of CIUK's defence strategy. CIUK relies on you to help it detect and contain Data Breaches at an early stage.

Here are a few indicators for potential Data Breaches that you should watch out for:

In the real world:

(a) Donors, trustees, supporters, volunteers or beneficiaries or other related data subjects notifying you that they received information which does not belong to them;

(b) Donors, supporters, volunteers or beneficiaries or other related data subjects telling you that they have been contacted by third parties and are wondering where these third parties got their contact details from;

(c) print outs of business documents in unsecured bins or unattended;

(d) unauthorised persons without escort in any CIUK premises or facilities; and

(e) Volunteers, trustees, or staff members asking for access to, or being in possession of, information they do not need to know.

In the IT world:

(a) unusually slow Internet or devices;

(b) locked out accounts or multiple failed login attempts;

(c) pop-ups and redirected websites when browsing;

(d) unexpected software installs;

(e) unexplained changes to files;

(f) large number of requests for the same objects or files or requests for a large number of objects or files;

(g) unknown/unauthorised IP addresses on wireless networks;

(h) unexplained system reboots or shutdowns; and

(i) services and applications configured to launch automatically.

If you become aware of any of these or similar suspicious circumstances, please report these to [the Compliance Team]. Don't assume that they already know or that an incident is not important. It is much better to report a trivial matter than not to report a critical one.

2. CIUK's Data Breach response procedure

CIUK's procedure in cases of Data Breach consists of responsive actions in the following phases:

(a) detection and first level reporting;

(b) initial response and second level reporting;

(c) investigation, containment and remedial measures;

(d) identification of reportable Data Breaches;

(e) notification of regulator / individuals affected;

(f) taking any other action required (e.g. ad-hoc reporting);

(g) incident review and documentation; and

(h) implementation of preventive measures.

Specific requirements of CIUK in relation to these phases are set out below.

3. Information required for notifications

CIUK requires that all Data Breach notifications to the ICO:

(a) describes the nature of the Data Breach (including where possible the categories and approximate number of: (i) data subjects concerned; and (ii) personal data records concerned);

(b) includes the name and contact details of CIUK's contact point (as applicable) who is able to supply further information;

(c) describes the likely consequences of the Data Breach; and

(d) describes the measures which CIUK has taken, or proposes to take, to address the Data Breach (including any measures to mitigate the possible adverse effects of the Data Breach).

If full details of the Data Breach are not available during the initial 72 hour period (i.e. where the Data Breach is complex and requires further forensic investigation to establish required details of the Data Breach), CIUK may provide an initial notification and follow-up with additional information during later phases as it becomes available.

The initial notification should set out what additional information will be provided at a later stage and provide reasons for the delay in providing full information. Authorised persons from [the IT, Legal and/or Compliance Department(s)] will liaise with the regulator and agree how and when the additional information will be provided.

4. Notifying the individuals concerned

In some circumstances CIUK may be required to notify individuals who are impacted by the Data Breach. CIUK requires that these notices are given in clear and plain language and:

(a) describe the nature of the Data Breach;

(b) include the name and contact details of CIUK's contact point (as applicable) who is able to supply further information;

(c) describe the likely consequences of the Data Breach; and

(d) describe the measures which CIUK has taken or proposes to take to address the Data Breach (including any measures to mitigate the possible adverse effects of the Data Breach).

The notification should also provide advice to individuals to protect themselves from possible adverse consequences of the Data Breach, for example resetting passwords.

CIUK requires that notification of a Data Breach is made to the affected individuals directly, unless this is not possible or would involve a disproportionate effort. Messages to the affected individuals should only concern the relevant Data Breach, and should not be sent with any other information such as a newsletter or product advertisements.

If direct communication is not possible, CIUK may issue a public communication. Examples of appropriate communication methods include: email, SMS and post (as means of direct communication); prominent website banners; and prominent advertisements in print media. CIUK will use a combination of different methods to maximise the chance of communicating to all of the affected individuals where appropriate and provide communications in relevant languages so affected individuals are able to understand the information.

CIUK may contact the regulator to seek guidance on the need to notify individuals and, if required, the most appropriate means to contact them.

5. Incident review and preventative action

Data Breach Documentation

CIUK requires that a record of all Data Breaches are kept, regardless of whether notified to the regulator or individuals concerned. These records include:

(a) the facts relating to the Data Breach (including the causes, what took place and the personal data affected) and its effects;

(b) the region in which the Data Breach occurred;

(c) any remedial action taken;

(d) the regulator to whom the Data Breach has been reported (if applicable);

(e) the steps taken to ensure that individuals likely to have been impacted by the Data Breach have been fully informed, including of their rights and support available to them (if any);

(f) the preventative actions being implemented to prevent similar Data Breaches in the future; and

(g) the reasons for any decisions taken in response to a Data Breach, in particular in relation to notification of supervisory authorities and individuals concerned as well as any relevant communications.