Pro-innovation Solutions

Date: 1st May 2018

Data Breach Response Procedure

Pro-innovation Solutions

Contents

Clause

Pro-innovation Solutions

Data Breach Response Procedure

1. About this Procedure

1.1 This procedure outlines the steps you must observe when processing Personal Data where you suspect or know that there has been a Data Breach.

1.2 This procedure applies to all employees, officers, consultants, contractors, volunteers, Apprentices casual workers, agency workers and anyone who has access personal data, whether or not you process it.

1.3 Misuse of personal data can not only damage the business and our reputation but it can result in a substantial fine from the Information Commissioners Office (ICO) of 20 million Euros or 4% of our worldwide turnover.

1.4 Breach of this Procedure will be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.5 This Procedure does not form part of any employee's contract of employment and we may amend it at any time.

2. Personnel Responsible for the Procedure

2.1 Our Director(s) has overall responsibility for the effective operation of this procedure and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the procedure and ensuring its maintenance and review has been delegated to the Data Protection Officer

2.2 Managers have a specific responsibility to ensure the fair application of this procedure and all members of staff are responsible for supporting colleagues and ensuring its success.

2.3 The IT Department and Provider will deal with requests for permission or assistance under any provisions of this procedure, and may specify certain standards of equipment or procedures to ensure security and compatibility.

3. What is a Data Breach?

3.1 A personal data breach means a breach of the security around that data which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3.2 It is an incident that affects the confidentiality, integrity or availability of personal data.

3.3 Both accidental and deliberate actions are considered breaches.

3.4 Examples include:

3.4.1 Access by an unauthorised person or third party;

3.4.2 Deliberate or accidental action (or inaction) by a company;

3.4.3 Sending personal data to the wrong person (including via email or post);

3.4.4 Computers, phones, tablets and other such devices which contain personal data, being lost or stolen;

3.4.5 Alteration of personal data without permission;

3.4.6 Loss of availability of personal data such as lost keys, forgotten passwords, or corrupted files.

4. Suspected Breaches

4.1 You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone else, other than in accordance with this Procedure.

4.2 If you suspect a data breach has taken place you must **immediately** inform the General Manager Where the General Manager is not contactable, you must inform the next most senior manager available to you.

4.3 Where possible, you should attempt to retrieve the data if emailed to the wrong person or placed in the post and it can be located.

4.4 To retrieve an email you should:

- open the sent message and locate the "*actions*" button at the top of the screen;
- Click on "actions" and within this there will be the option to "Recall this message";
- Click on this option and follow the steps on screen to "delete unread copies if this message" as soon as possible.
- Where a recall is successful, you will receive a notification.
- Whether or not you are successful, you must inform the General Manager of the result.

5. Reported Breaches

5.1 Where a breach or suspected breach, is reported, the General Manager will review what happened and determine whether there has been a breach at all.

5.2 The General Manager will take all necessary and available steps to retrieve, recover or fix the data breach. All staff must assist the General Manager as much as possible in order to lessen the effect of the breach.

5.3 For example:

5.3.1 If a computer has been lost, the General Manager will check if it was password protected. If possible the IT provider will remotely wipe any data from the device to stop continuation of the breach.

5.3.2 If a person has accessed a part of the computer system without authority, all related passwords will be changed.

6. Record of Breaches

6.1 All suspected breaches will be recorded by the General Manager and any necessary steps to avoid a future breach of the same kind, will be considered and implemented.

6.2 Where a breach has taken place, that is not notifiable to the ICO and data subject, the General Manager will make a record of the breach which will include;

- What happened;
- Who was involved;
- How it happened;
- What steps were taken to resolve the breach;
- What decisions were taken in relation to reporting the breach.

7. Notification of Breaches to Data Subject

7.1 Where the breach is likely to result in a high risk to the rights and freedoms of the data subject, the data subject **will be notified** of the breach.

7.2 The General Manager will investigate and determine whether the breach is unlikely to result in a risk to the rights and freedoms of the data subject. If so, no notification will be sent and a record of this decision will be made which will include the details set out in clauses 6 above.

7.3 When the data subject is notified of a breach, they will be told in clear, plain language:

- The nature of the data breach;
- The name and contact details of the General Manager
- A description of the likely consequences of the breach; and
- A description of the steps taken or planned, to deal with the data breach.

8. Reporting Breaches to the ICO

8.1 When a breach occurs that is considered likely to cause risk to the data subject, the breach **must** be reported to the ICO within 72 hours where feasible. This is known as a notifiable breach.

8.2 All decisions in relation to breaches will recorded and such records maintained and stored by the General Manager

8.3 Reporting a breach to the ICO must include:

8.3.1 A description of the nature of the breach including the types of people and number of people affected and the types of data and number of records concerned;

8.3.2 The name and contact details of the General Manager

8.3.3 A description of the likely consequences of the breach; and

8.3.4 A description of the steps taken or planned in order to deal with the data breach.

8.4 Reports can be made online at www.ico.org.uk or via the ICO telephone number **0303 123 1113.**

9. Review of Breaches

9.1 Once an investigation (and reporting where applicable) of a breach is complete, the General Manager will review what happened and consider and implement any steps/processes which need to be taken to ensure that the same does not happen again.

9.2 If the breach is due to the deliberate actions of anyone listed in clause 1.2 above, disciplinary action may be taken in accordance with the company disciplinary policy. Such action may include summary dismissal for gross misconduct.