General Data Protection Regulations - GDPR

DATA BREACH POLICY

1. INTRODUCTION

1.1 Data subjects have certain rights in respect of their personal data. When we process data subjects' personal data, we shall respect those rights. This policy and its appendices provide a framework for dealing with data breaches. It is our policy to ensure that data breaches in respect of personal data are handled in accordance with applicable law.

2. DEFINITIONS

2.1 For the purposes of this policy, the following terms have the following meanings:

Data: is information which is stored electronically, or in certain paper-based filing systems.

Data subjects: means all living individuals about whom we hold personal information

Personal data: means any information relating to an identified or identifiable data subject. An

identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier.

DPO: Data Protection Officer

Data controllers: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the data controller of all personal data used in our business for our own commercial purposes.

Data processors: are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

GDPR: The General Data Protection Regulations

ICO: The Information Commissioner's Office

Processing: is any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

3. ABOUT THIS POLICY

3.1 This policy outlines what action we will take and within what time frames if we become aware of a data breach in respect of personal data, to ensure we are compliant with data protection law (in particular the GDPR) and best practice.

3.2 The appendices to this policy should be used as follows:

Appendix One: for a breach that is notifiable to the ICO;

Appendix Two: for a breach that is notifiable to affected data subjects;

Appendix Three: to record all breaches and actions and decisions taken in relation to them.

4. REPORTABLE BREACHES

4.1 Types of breach that may be reportable under the GDPR include the following:

4.1.1 when data is accidentally or unlawfully destroyed;
4.1.2 when data is lost;
4.1.3 when data is accidentally or unlawfully altered;
4.1.4 when data is accessed by an unauthorised person;
4.1.5 when data is corrupted.

4.2 Data breaches must be reported to the ICO where it is likely that there will be a risk to people's rights and freedom. The ICO states that this includes physical, material or non-material

damage such as loss of control over personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

4.3 Data breaches must also be reported to the affected individual if there is a high risk of adversely affecting the individual's rights and freedoms.

5 TIME LIMITS FOR REPORTING

5.1 Data breaches falling under 4.2 must be reported to the ICO within 72 hours where feasible.

5.2 Data breaches falling within 4.3 must be reported to the affected individual without delay.

6 RESPONSIBILITIES OF THE DPO OR PERSON WITH RESPONSIBILITY FOR THE OPERATION OF THIS POLICY

6.1 The DPO or person with responsibility for the operation of this policy ("the Responsible Officer") shall take the following actions on being notified of a potentially reportable breach:

6.1.1 record the breach in the Data Breach Register (Appendix Three);

6.1.2 evaluate the breach to see whether it falls within either or both of 4.2 and 4.3 above and take the appropriate action within the appropriate time scale using the template documents in Appendices One and Two as appropriate;

6.1.3 investigate the circumstances of the breach and record details of the investigation for providing to the ICO;

6.1.4 consider possible consequences and adverse effects of the breach;

6.1.5 consider what steps the business can take to mitigate any adverse effects of the breach for individuals affected by it;

6.1.6 consider what advice if any should be provided to affected individuals to help them to protect themselves from the effect of the breach

6.1.7 consider any further remedial action that the business should take in relation to the breach including notifying and/or training affected staff;

6.1.8 consider whether any of the following should be notified and act accordingly: overseas data protection authorities; the police; any other regulatory bodies;

6.1.9 record any reasons for delay in reporting the breach, whether to the ICO or to affected individuals;

6.1.10 record all actions and decisions in relation to the breach and specifically those referred to above in the Data Breach Register, including any decision taken not to report the breach and the reasons for such decision.

Appendix 1

Data Security Breach Notification to the ICO

[On headed notepaper of data controller]

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

[DATE]

Dear Sirs,

Notification of a serious data security breach

I am writing to notify you of a [breach of security that resulted in the [loss **OR** unauthorised disclosure **OR** corruption **OR** destruction] of personal data. We consider this to be a serious data security breach.

[We have investigated the breach by [DETAILS OF HOW THE BREACH WAS INVESTIGATED] and provide you with the following information.]

[We are in the process of investigating the breach and we anticipate completing our investigation by [DATE], when we will provide you with the further information required. We can provide you with the following details at this stage [PROVIDE AS MUCH INFORMATION AS POSSIBLE UNDER THE FOLLOWING HEADINGS (SEE BELOW) AND IF INCOMPLETE PROVIDE DETAILS OF WHEN YOU EXPECT TO BE ABLE TO PROVIDE THE INFORMATION: CONTACT DETAILS; PERSONAL DATA PLACED AT RISK; CONTAINMENT AND RECOVERY.]

DETAILS OF THE DATA SECURITY BREACH

The name of the organisation is [NAME OF ORGANISATION] [and it is the data controller in respect of the data breach. The data protection registration number is [NUMBER]].

[I am sorry for the delay in reporting this incident to you but this was because [REASONS].]
The breach was discovered on [DATE] and is likely to have taken place on [DATE].

The information has been [accidentally or unlawfully destroyed **OR** lost **OR** altered **OR** disclosed without authorisation **OR** accessed by [[NAME OR DESCRIPTION OF ORGANISATION] **OR** an unauthorised person]].

The breach occurred under the following circumstances and for the following reasons:

- [CIRCUMSTANCES].
- [REASONS].

MEASURES IN PLACE

We had the following measures in place to prevent an incident of this nature occurring:

- [MEASURES].

We enclose extracts of policies and procedures that we consider to be relevant to the breach:

- [EXTRACTS OF POLICES AND PROCEDURES AND DATE IMPLEMENTED].

The following were in existence at the time of the breach:

- [LIST OF POLICIES AND PROCEDURES AND DATE IMPLEMENTED].

PERSONAL DATA PLACED AT RISK

The breach affects the following types of information:

- [TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL OR SPECIAL CATEGORY/SENSITIVE PERSONAL DATA AND DETAILS OF THE EXTENT].

It is likely that the breach affects around [NUMBER] data subjects.

[We have [not] informed the individuals affected by the breach because [REASONS FOR DECISION] **OR** The individuals are [aware **OR** unaware] that the incident has occurred].

The breach may have the following consequences and adverse effects on the affected data subjects:

- [CONSEQUENCES].
- [ADVERSE EFFECTS].

We have [received [NUMBER] of complaints **OR** not received any complaints] from the affected individuals.

CONTAINMENT AND RECOVERY

We [have taken **OR** propose to take] the following measures to address the breach and to minimise and mitigate its effects on the affected individuals:

- [MEASURES].

The information has [not] been recovered [and the details are as follows:

- [DETAILS OF HOW AND WHEN IT WAS RECOVERED].]

We have also taken the following steps to prevent future occurrences of the breach:

- [REMEDIAL ACTION TAKEN].
- [The facts surrounding the breach, the effects of that breach and the remedial action taken have been recorded in a data breach register maintained by the [data controller **OR** the company].]

TRAINING AND GUIDANCE

We do [not] provide staff with training on the requirements of the General Data Protection Regulations [and the details are as follows:

- [DETAILS OR EXTRACTS FROM TRAINING MANUALS RELEVANT TO THIS DATA BREACH].]

We do [not] provide detailed guidance to staff on the handling of personal data in relation to this incident [and the details are as follows:

- [DETAILS OR EXTRACTS OF ANY DETAILED GUIDANCE GIVEN TO STAFF ON THE HANDLING OF PERSONAL DATA IN RELATION TO THE DATA BREACH].]

We confirm that training on the requirements of the General Data Protection Regulations is [not] mandatory for all staff [and that the staff members involved in this incident received training on [DATE]].

PREVIOUS CONTACT WITH THE INFORMATION COMMISSIONER'S OFFICE

We have [not] reported [any] previous incidents to you within the last two years [and the details and reference numbers are as follows:

- [DETAILS OF INCIDENT(S)].
- [DATE(S) ON WHICH THE INCIDENT(S) WAS [WERE] REPORTED].
- [THE INFORMATION COMMISSIONER'S REFERENCE NUMBER(S), IF KNOWN].]

MISCELLANEOUS

We have [not] notified any other (overseas) data protection authorities about this data breach [and the details are as follows:

- [DETAILS OFDATA PROTECTION AUTHORITIES].]

We have [not] informed the police about this data breach [and the details are as follows:

- [DETAILS AND NAME OF POLICE FORCE].]

We have [not] informed any other regulatory bodies about this data breach [and the details are as follows:

- [NAME AND DETAILS OF REGULATORY BODIES].]

There has [not] been [any] media coverage [and the details are as follows:

- [DETAILS OF MEDIA COVERAGE].]

In addition, we consider that the following information would be of interest to you:

- [DETAILS].

CONTACT DETAILS

If you require any further information about the breach, please contact:

- [CONTACT NAME]
- [NAME OF DATA CONTROLLER]
- [POSTAL ADDRESS]
- [TELEPHONE NUMBER]
- [E-MAIL ADDRESS]
- [WEBSITE ADDRESS].

Yours faithfully,

[Name]

For and on behalf of [Data Controller]

Appendix 2

Data Security Breach Notification to the Data Subject

[On headed notepaper of data controller]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Dear [DATA SUBJECT],

Notification of a personal data security breach

We are sorry to inform you of a breach of security that has resulted in the [loss **OR** unauthorised disclosure **OR** destruction **OR** corruption] of your personal data.

The breach was discovered on [DATE] and is likely to have taken place on [DATE].

As a result of our investigation of the breach, we have concluded that:

- The breach affects the following types of information:
  - [TYPES OF INFORMATION. FOR EXAMPLE, FINANCIAL, SPECIAL CATEGORY/SENSITIVE PERSONAL DATA].
- The information has been [accidentally or unlawfully destroyed **OR** lost **OR** altered **OR** disclosed without authorisation **OR** accessed by [[NAME OR DESCRIPTION OF ORGANISATION] **OR** an unauthorised person]].
- The breach occurred under the following circumstances and for the following reasons:
  - [CIRCUMSTANCES].
  - [REASONS].

We have taken the following steps to mitigate any adverse effects of the breach:

- [MEASURES].

We recommend that you take the following measures to mitigate possible adverse effects of the breach:

- [MEASURES].

[We informed the Information Commissioner's Office of the breach on [DATE]].

You can obtain more information about the breach from any of the following contact points:

- [DATA CONTROLLER'S NAME].
- [DATA CONTROLLER'S POSTAL ADDRESS].
- [DATA CONTROLLER'S E-MAIL ADDRESS].
- [DATA CONTROLLER'S [TELEPHONE NUMBER **OR** HELPLINE NUMBER].
- [DATA CONTROLLER'S WEBSITE ADDRESS].

We apologise for any inconvenience this breach may cause you.
Yours sincerely,

[NAME]

For and on behalf of [DATA CONTROLLER]

Appendix 3

Data Breach Register

[Data Controller] GDPR Breach Register

Date of entry on Register	Matter Ref	Reported by	Time & Date of Internal Breach	Description of Breach and individuals involved	Time & Date of Report to ICO	If not reported to ICO, reason why not	Details of Report to Affected Data Subjects if appropriate

eventwest

