Everest People

Data Breach Policy

This Policy is issued by:	Everest Limited (referred to below as 'the Company)
The Responsible Person for this Policy is:	Nikki Johnson
The Data Protection Officer is:	Karl Munns
The Data Security Officer is:	Nikki Johnson

1. INTRODUCTION

1.1. The Company has adopted this Policy to comply with the Data Protection Legislation, which requires it to report certain types of Personal Data Breach to the Information Commissioner's Office (ICO).

1.2. Where a Data Breach presents a high risk to data subjects' rights and freedoms, the Company must also notify these individuals and do so without delay.

1.3. The objectives of this Policy are to:

- Comply with the Data Protection Legislation
- Protect the rights of the Data Subjects whose Personal Data we process
- Provide openness and transparency
- Demonstrate accountability in relation to the data protection principles

1.4. The Company has a very short period of time in which to investigate and act to report Data Breaches, so the steps detailed below must be taken as quickly as possible. Unreasonable delay or inaction will be treated as a breach of this Policy and may result in disciplinary action because the potential adverse consequences for Data Subjects and the Company are very serious.

1.5. Please refer to the list of defined terms at the end of this Policy and note that all title case terms have specific meanings in the context of this Policy.

2. KEY INDIVIDUALS

2.1. The Data Security Officer is responsibility for managing Data Breaches.

2.2. If for any reason the Data Security Officer is unavailable, then contact one of the Data Protection Officer or the Chief Executive.

2.3. If none of these people are available, the most senior manager available will ensure this Policy is adhered to.

3. WHAT IS A DATA BREACH?

3.1. A Data Breach is any breach of security (either physical or cyber) that leads to any of the following:

- Destruction or loss of Personal Data (whether by accident or intent)
- Unauthorised alteration to Personal Data
- Disclosure of Personal Data to any unauthorised person or organisation
- Access by someone who is not properly authorised to access
- Corruption to Personal Data such that access is made impossible

3.2. These types of events constitute a Data Breach whether the data is held or transmitted electronically or in hard copy. It is also a Data Breach if the data is copied and the copy is taken outside of the Company's possession or control (so that the original data remains in place and is otherwise unaffected).

4. TYPES OF EVENTS THAT ARE LIKELY TO CONSTITUTE A DATA BREACH

4.1. It is important to be mindful of the types of events that will constitute a Data Breach and to keep a look out for things that either suggest one of these has happened, or that one of these is likely to happen.

4.2. A Data Breach is broadly any event that causes Personal Data that is controlled by the Company to no longer exist, or to no longer exist in a form that can be used as intended. It also includes events where Personal Data is altered, corrupted, is no longer complete or is copied in an unauthorised way.

4.3. This is a non-exhaustive list of examples (in no particular order):

- Computer or network hacked or infected with malware or ransomware
- Correspondence (email or hard copy) sent to incorrect recipient
- Documents in hard copy disposed of improperly (i.e. not placed in confidential shredding)
- Company device lost, stolen or mislaid
- Client contact details copied to, or stored on, a device other than a Company device
- Files or documents damaged so that data cannot be read or retrieved
- Photographs of Company data taken by an unauthorised person
- Accidental deletion of files by company personal
- Data is encrypted, and the encryption key is not in the Company's possession

4.4. You may become aware of the circumstances yourself, or be made aware of the circumstances from:

- a Data Subject;
- one of the Company's Data Processors;
- a member of the public;
- a member of Company Personnel;
- or one of the Company's business partners or other stakeholders.

4.5. Please also be mindful of your personal responsibility to report a breach no matter how the circumstances came to your attention; do not assume that someone else has reported, or will report, the circumstances. We would rather circumstances were reported multiple times, than risk them not being reported at all.

5. WHAT TO DO IF YOU BECOME AWARE OF OR SUSPECT A DATA BREACH

5.1. All Company Personnel have an individual and shared responsibility to report events that suggest a Data Breach may have occurred.

5.2. It is not necessary or appropriate for you to investigate any circumstances that indicate a breach may have taken place, you need only report them to the key individual (see above). You should also notify your manager.

5.3. Request an acknowledgement of your email notification and make a note to follow up with further action to report if you do not receive an acknowledge of receipt: within 3 working hours if your report is made within normal working hours, or otherwise by midday on the day following your report.

5.4. If there is something you can do quickly to prevent loss or damage, or further loss or damage, (without risk to your own safety, health or wellbeing) then you should take such action first, and then act immediately to report the circumstances.

5.5. Do not rely only on email when reporting a suspected Data Breach but also report by phone to both the key individual and your manager.

5.6. If you cannot reach either the key individual or your manager by phone, use every reasonable means of contacting them immediately.

5.7. You should also contact the police if the circumstances you become aware of also constitute a criminal offence (e.g. unlawful damage to property, burglary or theft) and where it is appropriate to do so. If you are in any doubt about this speak to the key individual first.

6. RESPONSE PLAN

6.1. The focus on the sections that follow is to establish quickly what has happened and the attendant risks to Data Subjects, and thereby to facilitate action to notify the ICO where appropriate and to protect Data Subjects from any adverse consequences of a Data Breach.

6.2. The key individual will take all reasonable action to contain any potential Data Breach and thereby limit the risk of any additional Data Breaches or loss of Personal Data.

6.3. This person will also take such steps as are reasonable within no more than 60 hours to establish the following:

6.4. **Validation:**

- Do the circumstances reported involve any data held by or on behalf of the Company that includes Personal Data?

6.5. **Investigation**

- Which of the Company's Data Assets are affected (or may have been affected) by the circumstances?
- What categories of Data Subject are potentially affected (e.g. children, vulnerable groups, those with disabilities, employees, customers, those the Company markets to, etc)?
- What categories of Personal Data are contained within the Data Asset(s) affected (e.g. health data, employment records, financial details, bank account numbers, passport numbers, etc)?
- Approximately how many records (i.e. individual files or database items) in the affected Data Asset(s) are affected?
- Approximately how many Data Subjects within each Data Asset have been potentially affected by the circumstances?
- Are the types of Personal Data contained within the Data Asset(s) likely to create a high risk of harm or prejudice to Data Subjects' rights or freedoms?
- Do the categories of Personal Data affected include Sensitive Personal Data?
- Are the Data Asset(s) affected encrypted or protected by password and/or other security measures and, if so, is this likely to render them inaccessible to any unauthorised person who may access them?

6.6. **Mitigation**

- What measures have been taken (or are proposed) to address any Data Breach?
- What measures have been taken (or are proposed) to mitigate the possible adverse effects of any Data Breach?
- Is any Personal Data pseudonymised so that the Data Subjects are not identifiable and, if so, can the pseudonymisation process be reversed by someone other than an authorised member of Company Personnel?
- Were the mitigating measures in place successful or partially successful in preventing any impact on Data Subjects?

6.7. Where necessary the key individual will seek the services of experts relevant to the circumstances of the Data Breach to assist in establishing the answers to the questions above. In most cases this will include both the Company's data consultancy supplier and when computer systems have been compromised the IT systems provider.

6.8. Where feasible statements will be taken from Company Personnel who have first-hand knowledge of the circumstances or other relevant facts.

6.9. Where there is contemporaneous documentation relevant to the circumstances or other relevant facts, this will be preserved. Similarly, if documentation can be generated from a computer or other system that is relevant, it will be generated and preserved.

7. REPORTING

7.1. The key individual will identify whether or not a Data Protection Impact Assessment has been undertaken that includes any analysis of risk in the circumstances of the Data Breach. If such an assessment has been carried out the Responsible Person will have reference to this in relation to this section of the Policy.

7.2. The Responsible Person, with such assistance from experts as may be appropriate, shall wherever feasible determine the following within 72 hours of becoming aware of the circumstances:

- whether the facts as they are apparent from the investigation show that one (or more) of the circumstances listed in the heading 'what is a data breach?' have taken place;
- If so, what effect this is likely to have on the Data Subjects' rights and freedoms, in particular whether or not it is likely to result in any Prejudice to those rights and freedoms.

7.3. The term 'Prejudice' shall include, but not be limited to, any of the following:

- Loss of control by the Data Subject over his/her Personal Data
- Limitation to the Data Subjects rights
- Discrimination against the Data Subject by others
- Identity theft or fraud in which the Data Subject may be the victim

- Financial loss by the Data Subject
- Unauthorised reversal of pseudonymisation of the Data Subject's Personal Data
- Damage to the Data Subject's reputation
- Loss of confidentiality of Personal Data that is protected by professional secrecy (either by unauthorised or accidental disclosure or otherwise)
- Any significant economic or social disadvantage
- Significant distress that exceeds what could be sensibly characterised as mere inconvenience

7.4. If the likely effect of the Data Breach includes Prejudice, then action must be taken to report the matter to the ICO within 72 hours of becoming aware of the circumstances. In this context 'aware' means that the Responsible Person has a reasonable degree of certainty that the reported event has led to Personal Data being compromised.

7.5. Only where the Data Breach is unlikely to present a risk to Data Subjects' rights and freedoms will it be appropriate not to notify the ICO. An example of this is where the Personal Data affected is already in the public domain.

7.6. If it is not possible to have fully investigated the Data Breach within 72 hours, so as to be able to determine the relevant facts then as much information as is available must be reported to the ICO within this time period and the remaining information must be provided as soon as possible.

7.7. If it is apparent that there has been a Data Breach that involves Prejudice, but the relevant facts cannot be accurately reported within 72 hours, then the ICO should be notified of this as soon as possible (i.e. wherever possible before the 72-hour deadline).

7.8. Serious breaches should be reported to the ICO's security breach helpline on 0303 123 1113 (open Monday to Friday 9am to 5pm). Select option 3 to speak to ICO staff who will be able to assist. Alternatively, notification should be in writing to 'casework@ico.org.uk' or by post to the ICO at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

7.9. As a minimum the report to the ICO must include the following:

- The nature of the Personal Data Breach (including, where possible, the categories of Data Subjects affected and the categories and approximate number of records concerned)
- The name and contact details of the Responsible Person
- The likely consequences of the Personal Data Breach
- The measures taken or proposed to be taken to address the Data Breach, including where applicable, measures to mitigate its possible effects

7.10. The ICO's security breach notification form is linked here.

7.11. If for any reason a Data Breach that involves Prejudice is not reported to the ICO within 72 hours, then a record of the reasons for the delay must be kept and the ICO informed of these when notification is made.

8. INFORMING DATA SUBJECTS

8.1. Where there is a high risk to the rights and freedoms of Data Subjects the Responsible Person shall notify the Data Subjects of the Data Breach as soon as possible so that they can take steps to protect themselves.

8.2. 'High risk' means that the severity of the Prejudice is high (e.g. the Data Breach involves the loss of Sensitive Data or data that can be used to defraud the Data Subjects) and the type of Prejudice identified is likely to result from the Data Breach.

8.3. In these cases, the ICO notification process will have taken place, or be underway, and the Responsible Person should take advice from the ICO about whether or not Data Subjects should also be informed.

8.4. Note that even when the Personal Data is encrypted (and the encryption security is not compromised), there may still be a high risk of Prejudice if the Data Subjects' Personal Data is no longer available for processing.

8.5. When Data Subjects are informed, the Responsible Person should give any practical advice that will minimise the risk to Data Subjects (e.g. to change their passwords or contact their banks).

8.6. Communication with the affected Data Subjects should also contain:

- The name and contact details of the Responsible Person or another point of contact where more information can be obtained
- A description of the likely consequences of the Data Breach
- Details of any measures taken (or proposed) to address the breach and reduce any impact on the Data Subjects

9. RECORD KEEPING

9.1. The Responsible Person must ensure that all Data Breaches and potential breaches are recorded in the Company's Data Breach Log, including those which do not need to be reported to the ICO or to Data Subjects.

9.2. The following information must be included in the Data Breach Log as a minimum:

- The cause of the Data Breach
- What took place in relation to the Data Breach
- The Personal Data that was affected
- The effects and consequences of the Data Breach
- Details of any action taken to remedy the Data Breach or mitigate its effects on Data Subjects
- A record of all decisions taken in relation to reporting and informing Data Subjects and the justification or reasons for those decisions.
- If the ICO is not informed within 72 hours, the reason why this did not happen

9.3. Copies of all statements and documentation will also be preserved and retained.

10. PROCESSORS

10.1. When the Company acts as Data Controller it is responsible for reporting Data Breaches by any Data Processor it uses. The Data Processor need only establish whether or not a breach has occurred and notify the Company (as Data Controller) of this. In this situation the Company is aware of the Data Breach when it has been notified by the Data Processor and the 72-hour time period runs from then.

10.2. The Company will ensure that the terms under which all Data Processors provide services reflect the Data Processor's obligations to inform the Company of any Data Breach without delay and fully co-operate in the response and reporting processes.

10.3. When the Company acts as Data Processor it acknowledges its duties toward the relevant Data Controller and will ensure that these obligations are reflected in the relevant terms and conditions.

11. ACTION TO AVOID SIMILAR CIRCUMSTANCES

11.1. An appropriate level of information regarding the circumstances of a Data Breach and any lessons learnt should be shared with others within the Company so that the risk of a similar occurrence is minimised.

11.2. When a Data Breach involves the Company's computer systems, IT expertise should be sought immediately and all appropriate action taken to prevent a similar occurrence and to minimise the loss of Personal Data.

11.3. In all cases involving a Data Breach the Company's data protection policies that relate to data security should be reviewed, amended as may be appropriate, and re-issued to all Company Personnel.

12. FURTHER GUIDANCE

12.1. The European Data Protection Board (EDPB)'s Guidelines on Personal Data Breach Notification linked here.

12.2. The ICO guidance on Personal Data Breaches linked here.

13. DEFINITIONS

13.1. The following defined terms are used in the context of this Policy.

- Company Personnel: all employees, workers, contractors, agency workers, volunteers and consultants who are engaged to work for the Company.
- Company Device: computer equipment including desktop, laptop and servers, mobile telephones, tablets, USB sticks and standalone hard drives or other data storage devices.
- Data Processor: an individual or organisation that processes information on behalf of a Data Controller.
- Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

- Personal Data: any piece of information which identifies a Data Subject, either directly or indirectly, alone or in combination with other data we can reasonably access, including any pseudonymised Data. Personal Data can be factual or consist of notes and opinions about a Data Subject. Any Personal Data that is processed by automated (electronic) means or as part of a structured filing system is covered by the Data Protection Legislation.