

Everest People

Data Retention Policy

This Policy is issued by:

Everest Limited
(referred to below as 'the Company')

The Responsible Person for this Policy is:

Karl Munns

The Data Protection Officer is:

Karl Munns

The Data Security Officer is:

Nikki Johnson



1. INTRODUCTION

- 1.1. The Data Protection Legislation requires those who processes the Personal Data of natural persons to do so according to the principles set under the General Data Protection Regulation (GDPR). This Policy refers specifically to one of those – the principle that data shall only be processed for as long as it is necessary for the purpose it was initially intended.
- 1.2. The GDPR does not set out any specific minimum or maximum periods for retaining Personal Data. Article 5 (1, e) states that Personal Data shall be: “kept in a form which permits identification of Data Subjects for no longer than necessary to the purposes for which the Personal Data are processed.”
- 1.3. To comply with this principle we:
 - Review the length of time we keep Personal Data
 - Consider our processing purpose/s when deciding whether (and for how long) to retain Personal Data
 - Securely delete information that is no longer needed for these purpose/s
 - Update, archive or securely delete information if it goes out of date
 - Think carefully about what data we wish to keep for internal monitoring and statistical purposes and ensure that wherever possible Personal Data in these records is removed

2. OVERVIEW

- 2.1. We adhere to this Policy to ensure that data is either securely deleted, minimised or anonymised when it is no longer needed for its intended purposes.
- 2.2. Some kinds of Personal Data are important for the Company’s internal management: to protect against any potential litigation; for the purposes of insurance claims; or to otherwise retain necessary records. In such cases retaining or processing data for longer periods is justified. Where this is the case, Personal Data will be kept for an appropriate period after the termination of any contract or business agreement, or other relationship with a Data Subject.
- 2.3. [Upon the expiry of the retention period for certain kinds of data which the Company still wishes to process for the purposes of maintaining historic records and / or archives, the Data will be anonymised. This means that no part of the Data can be used to identify a Data Subject, including the erasure of basic contact details, any unique identifiers which attribute the data to a natural person, and any piece of data which could be used to identify an individual if combined with other reasonably available data.]
- 2.4. Data retention periods shall be specific to the types of data being held and are outlined in the Company’s Schedule of Data Retention Periods below. These will be determined with reference to applicable legal bases and our legitimate interests.
- 2.5. Where Data is necessary to comply with legal requirements other than the Data Protection Legislation, the Company shall retain such Data for at least this period and will have reference to:

- Trade, tax, employment and administrative law
 - Regulators' Codes of Conduct and suggested retention periods
 - The Limitations Act 1980
- 2.6. In the absence of any legal requirement, the Company shall retain Personal Data only for as long as necessary to fulfil the specified purpose(s) for processing plus a reasonable additional period to provide a buffer and time for administration processes to be undertaken.
- 2.7. Every effort will be made to ensure the erasure of data when the data is no longer necessary to fulfil its specified purpose.

3. RESPONSIBLE PERSONS

- 3.1. The Data Protection Officer is responsible for ensuring this policy is adhered to.
- 3.2. The Company's senior managers also have responsibility to ensure compliance in their respective areas.
- 3.3. The Company's senior managers have the authority to:
- Monitor departmental compliance with the Data Protection Legislation
 - Restrict employees' access to certain kinds of data
 - Purge any Company database of expired data

4. DATA RETENTION PROCEDURES

- 4.1. The Company adopts an organised approach to attributing appropriate data retention periods to the data it processes about Data Subjects.
- 4.2. This approach shall be adhered to by all employees responsible for creating and organising databases containing personal information.
- 4.3. Any new database will be formatted or otherwise organised in a manner which allows for the labelling of data retention periods, or expiry dates onto data records.
- 4.4. Reasonable steps will be taken to amend the format of existing databases to allow for labelling as above.
- 4.5. We ensure retention periods are complied with by:
- [a scheme of retention codes to allow for ease of identifying how long captured data should be stored]
 - [automated purging of electronic records and files]
 - [periodic purging of documentation, e.g. forms, reports, emails and correspondence]

5. DATA DELETION PROCEDURES

- 5.1. The Company shall ensure it takes all appropriate measures to delete or destroy any data which is no longer lawfully held according to the retention period associated with its intended purpose of processing.

- 5.2. It shall use any reasonably available automated means of deleting data or imposing an alert system to flag up expired data on the Company's systems wherever feasible.
- 5.3. Our managers shall be tasked to ensure the destruction of paper files whose retention period has expired and to do so on a regular basis, using such methods as:
- separating out completed working documents from those that remain active
 - regular review of inactive clients
 - maintenance of a journal of expiring data to conduct a comprehensive data purge at regular intervals

6. SCHEDULE OF RETENTION PERIODS

- 6.1. The Company shall adopt the retention periods in the schedule that follows to ensure Personal Data is retained only for as long as necessary to fulfil its intended purpose.