

## Everest People

### Data Subject Rights 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. Individuals ('Data Subjects') have certain rights in respect of the information we hold about them (their 'Personal Data'). When we process this Personal Data we respect those rights, and the procedures below provide a framework for responding to requests by individuals to exercise those rights.
- 1.2. 'Personal Data' includes any information relating to a living person who can be identified either directly, or in combination with other data which we hold or could reasonably access.
- 1.3. 'Processing' includes any operation or set of operations performed on Personal Data, such as collection, use, storage, dissemination and destruction.
- 1.4. 'Data Subject' means a living identifiable individual about whom we hold Personal Data.
- 1.5. 'Personal Data' (or 'Data') means any information which can identify a natural person either directly or indirectly, alone or in combination with other data. For the purposes of this Policy, the only Personal Data which is captured by the Data Protection Legislation is that which is processed by automated electronic means, or which is organised in any kind of structured filing system which can be searched and individuals found by using specific criteria.
- 1.6. These procedures only apply to Data Subjects who are either residents or nationals of any country in the European Economic Area, and whose Personal Data we process as part of an automated or structured filing system.

## 2. RESPONDING TO REQUESTS TO ACCESS PERSONAL DATA

- 2.1. Data Subjects have the right to request access to their Personal Data processed by us, either directly, or via a Power of Attorney or other duly authorised legal representative.
- 2.2. Such requests are called Subject Access Requests (SARs). When a Data Subject or their representative makes a SAR, we shall take the following steps:
  - ensure the process is handled by an appropriate Responsible Person within the Company, or by an internal or external Data Protection Officer
  - log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
  - [invite, but not insist, the Data Subject to make their request via a template form to capture all the information we require to complete the request as quickly as possible]
  - where appropriate invite, but not insist, the Data Subject to narrow their request for particular kinds of data to aid in our search
  - confirm the identity of the individual making the request (we may refuse any request from an individual who does not adequately prove their identity)
  - confirm that we do process information about the requester and that they are a genuine Data Subject
  - where necessary search all available databases, systems, applications and other resources where the Data Subject's Personal Data may be held

- review the Personal Data and where it is necessary to do so redact or remove any Personal Data belonging to any other Data Subject
  - provide the specific requested data or all available data depending on the request
  - log the process from start to finish on all relevant internal logging systems
- 2.3. If Personal Data of the Data Subject are being processed, we shall provide the Data Subject with a completed SAR response letter, providing access to the following information:
- the purposes of the processing
  - the categories of Personal Data concerned
  - the recipients or categories of recipient to whom the Personal Data have been or will be disclosed
  - where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period
  - the existence of the right to request rectification or erasure of Personal Data or restriction of processing of Personal Data or to object to such processing
  - the right to lodge a complaint with the Information Commissioner's Office (ICO)
  - where the Personal Data are not collected from the Data Subject, any available information as to their source
  - the existence of any automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject, and
  - where Personal Data are transferred outside the EU, details of the appropriate safeguards to protect the Personal Data.
- 2.4. We shall, unless there is an exemption (see Paragraph 9 below), provide the Data Subject with a copy of the Personal Data that we process in a commonly used electronic form (unless the Data Subject has specifically requested to be provided with a copy in another form).
- 2.5. Copies of any information provided to the Data Subject shall be provided within one month of the receipt of the request.
- 2.6. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the Data Subject within one month of receipt of the request and explain the reason for the delay.
- 2.7. If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the Personal Data, or refuse to act on the request.
- 2.8. If we are not going to respond to the SAR we shall inform the Data Subject of the reason(s) for not acting and of the possibility of lodging a complaint with the ICO.

### **3. RESPONDING TO REQUESTS TO RECTIFY PERSONAL DATA**

- 3.1. Data Subjects have the right to have their Personal Data rectified where the data are incomplete or manifestly inaccurate. Data Subjects may provide a supplementary statement regarding the data to inform us of any inaccuracies or changes which must be made. Where such a request is made, we shall, unless there is an exemption (see Paragraph 9 below), rectify the Personal Data without undue delay.
- 3.2. We shall also communicate the rectification of the Personal Data to each recipient to whom the Personal Data have been disclosed unless this is impossible or involves disproportionate effort.

### **4. RESPONDING TO REQUESTS FOR THE ERASURE OF PERSONAL DATA**

- 4.1. Data Subjects have the right, in certain circumstances, to request that we erase their Personal Data.
- 4.2. We are required by law to honour such a request if one of the following applies (unless there is an exemption detailed in Paragraph 9):
  - the Personal Data are no longer necessary for the purposes they were originally collected
  - the Data Subject withdraws their consent to processing and there is no other legal basis for processing
  - the Data Subject objects to the processing provided the legal basis for processing is either Art5.1(e) public interest or (f) necessary for legitimate interests, and that there is no compelling reason why our interests should override those of the Data Subject
  - the Data Subject objects to the processing of their Personal Data for direct marketing purposes, with no exception
  - the Personal Data have been unlawfully processed;
  - erasure is required to comply with a legal obligation, or;
  - the Personal Data belong to a child under 16 and are processed in relation to an online service
- 4.3. When a Data Subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see Paragraphs 4.5 and 9 below), take the following steps:
  - log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met)
  - confirm the identity of the Data Subject who is the subject of the Personal Data. We may request additional information from the Data Subject to do this
  - search databases, systems, applications and other places where the Personal Data which are the subject of the request may be held and erase such data within one month of receipt of the request
- 4.4. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for

responding we shall inform the Data Subject within one month of receipt of the request and explain the reason(s) for the delay.

- 4.5. We will inform those who are processing the Personal Data that the Data Subject has requested the erasure by them of any links to, or copies or replications of the Personal Data.
- 4.6. We will also communicate the erasure request to each recipient to whom the Personal Data have been disclosed unless this is impossible or involves disproportionate effort.
- 4.7. If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.
- 4.8. If we are not going to respond to the request, we shall inform the Data Subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.
- 4.9. In addition to the exemptions in Paragraph 9 below, we can also refuse to erase the Personal Data to the extent processing is necessary:
  - for exercising the right of freedom of expression and information
  - for compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us
  - for reasons of public interest in the area of public health
  - for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
  - for the establishment, exercise or defence of legal claims

## **5. RESPONDING TO REQUESTS TO RESTRICT THE PROCESSING OF PERSONAL DATA**

- 5.1. Data Subjects have the right, unless there is an exemption (see Paragraph 9 below), to restrict the processing of their Personal Data if:
  - the Data Subject contests the accuracy of the Personal Data (for a period to allow us to verify the accuracy of the Personal Data)
  - the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead
  - we no longer need the Personal Data for the purposes we collected them, but they are required by the Data Subject for the establishment, exercise or defence of legal claims
  - the Data Subject has objected to the processing, pending verification of whether we have legitimate grounds to override the Data Subject's objection
- 5.2. Where processing has been restricted, we shall only process the Personal Data (excluding storage):

- with the Data Subject's consent
  - for the establishment, exercise or defence of legal claims
  - for the protection of the rights of another person
  - for reasons of important public interest
- 5.3. Prior to lifting the restriction, we shall inform the Data Subject of the lifting of the restriction.
- 5.4. We shall communicate the restriction of processing of the Personal Data to each recipient to whom the Personal Data have been disclosed, unless this is impossible or involves disproportionate effort.

## **6. RESPONDING TO REQUESTS FOR THE PORTABILITY OF PERSONAL DATA**

- 6.1. Data Subjects have the right, in certain circumstances, to receive their Personal Data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another Data Controller.
- 6.2. Where such a request is made, we shall, unless there is an exemption (see Paragraph 9 below), provide the Personal Data without undue delay if:
- the legal basis for the processing of the Personal Data is consent or pursuant to a contract; and
  - our processing of those data is automated.
- 6.3. When a Data Subject makes a request for portability in the circumstances set out above, we shall take the following steps:
- log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met)
  - confirm the identity of the Data Subject who is the subject of the Personal Data. We may request additional information from the Data Subject to confirm their identity
  - search databases, systems, applications and other places where the Personal Data which are the subject of the request may be held
  - provide the Data Subject with such data (or, at the Data Subject's request, transmit the Personal Data directly to another Company, where technically feasible) within one month of receipt of the request.
- 6.4. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months.
- 6.5. If we extend the period for responding we shall inform the Data Subject within one month of receipt of the request and explain the reason(s) for the delay.
- 6.6. If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the Personal Data, or refuse to act on the request.
- 6.7. If we are not going to respond to the request, we shall inform the Data Subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

## **7. RESPONDING TO OBJECTIONS TO THE PROCESSING OF PERSONAL DATA**

- 7.1. Data Subjects have the right to object to the processing of their Personal Data where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the Data Subject's interests or fundamental rights and freedoms, unless we either:
- can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or
  - are processing the Personal Data for the establishment, exercise or defence of legal claims.
- 7.2. Data Subjects also have the right to object to the processing of their Personal Data for scientific or historical research purposes, or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
- 7.3. Where such an objection is made, we shall, unless there is an exemption (see Paragraph 9 below), no longer process a Data Subject's Personal Data.
- 7.4. Where Personal Data are processed for direct marketing purposes, Data Subjects have the right to object at any time to the processing of their Personal Data for such marketing. If a Data Subject makes such a request, we shall stop processing the Personal Data for such purposes.

## **8. RESPONDING TO REQUESTS NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING**

- 8.1. Data Subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their Personal Data, if such decision produces legal effects concerning them or similarly significantly affects them.
- 8.2. Where such a request is made, we shall, unless there is an exemption (see Paragraph 9 below), no longer make such a decision unless it:
- is necessary for entering into, or the performance of, a contract between us and the Data Subject\*
  - is authorised by applicable law which lays down suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests
  - is based on the Data Subject's explicit consent\*
- 8.3. \*in these cases we shall implement suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

## **9. EXEMPTIONS**

- 9.1. Before responding to any request, we shall check whether there are any exemptions that apply to the Personal Data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above to safeguard:
- public security

- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
- other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions
- the protection of the Data Subject or the rights and freedoms of others; or
- the enforcement of civil law claims.