Everest People

Privacy Standard

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. Correct and lawful treatment of Personal Data maintains confidence in the organisation and provides for successful business operations.

1.2. Protecting the confidentiality and integrity of Personal Data is a business-critical responsibility.

2. GUIDANCE

2.1. Company Personnel seek advice in the following circumstances:

- if they are unsure about what security or other measures they need to implement to protect Personal Data
- if they have any information that is relevant to a Data Breach
- if they need any assistance dealing with any rights invoked by a Data Subject
- whenever they are engaging in a significant new processing activity which is likely to require a Data Protection Impact Assessment
- if they feel they have to use Personal Data for purposes others than what it was collected for
- If they plan to undertake any activities involving Automated Processing
- If they need help complying with applicable law when carrying out direct marketing activities
- if they need help in relation to our sharing of Personal Data with third parties

3. PERSONAL DATA PROTECTION PRINCIPLES

3.1. We adhere to these principles whenever we to process Personal Data:

- *Lawfulness, Fairness and Transparency*: The Data is processed within the terms of the Data Protection Laws, fairly and in a manner which enables accountability and compliance with Data Protection rights.
- *Purpose Limitation*: The Data is collected only for specified, explicit and legitimate purposes.
- *Data Minimisation*: The Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- *Accuracy*: The Data is accurate and kept up to date where necessary.
- *Storage Limitation*: The Data is not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Data is Processed.
- *Security, Integrity and Confidentiality*: The Data is Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- *Transfer Limitation*: The Data is not transferred to any another country without appropriate safeguards being in place.
- *Data Subjects' Rights and Requests*: The Data is made available to Data Subjects and they are able and assisted in exercising certain rights in relation to their Personal Data.

- *Accountability*: We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

4. LAWFULNESS, FAIRNESS, TRANSPARENCY

4.1. Company Personnel may only collect, process and share Personal Data fairly and lawfully and for specified purposes.

4.2. The Data Protection Laws restricts the processing of Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing, but to ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

4.3. Whenever we collect or process Personal Data we ensure it is necessary for one of the following reasons:

- to fulfil a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- to pursue our legitimate interests, which have been set out in a Privacy Notice to the Data Subject, and where the purpose for processing does not prejudice the interests or fundamental rights and freedoms of Data Subjects;
- the Data Subject has given their Consent.

4.4. We identify and document the legal grounds for each of our processing activities.

5. CONSENT

5.1. When no other legal basis can be relied upon to process Data that is necessary for our activities, we will seek the Consent of the Data Subject. We do not seek request to process personal data when another legal basis for processing is relied upon because this would mislead the data subject about the legal basis for the processing activity.

5.2. Company Personnel only ever obtain consent by using one of the Company's approved forms.

5.3. Company Personnel understand that the conditions of a consent being genuine and lawful require that it fulfils the following criteria:

- *Freely given*: We give the Data Subject the option to provide consent but there is no obligation for them to provide it.
- *Unambiguous*: The consent form requests a clear and affirmative action by the Data Subject, so there can be no doubt that they are actually granting their consent.
- *Specific*: We use 'granular' consents, which means we get separate consents for separate processing activities and avoid vague or blanket consents.
- *Separate*: The Consent are not contained in other agreements the Data Subject enters into with us.

- *Informed*: The Data Subject: knows who the Data Controller is (or if there are more than one, the names of all Data Processors), has been told about the purpose of each processing activity for which consent is sought, knows what type of Data is being collected and used, has been informed of their right to withdraw consent, has been told if the Data is to be used for automated decision making and has been told about the possible risks of any transfers to countries outside the EU.
- *Explicit* (in the case of Special Categories): The consent is confirmed in writing (and ideally signed in manuscript or electronically) or by the Data Subject filling in an electronic form or confirmed by a two-stage verification process.

5.4. A request from a Data Subject to withdraw consent will be honoured without delay and we ensure that withdrawing consent is as easy as proving it.

5.5. If the purpose of processing a Data Subject's information changes at any time, to any purpose which the Data Subject has not consented to, the Consent will be refreshed by contacting the Data Subject.

5.6. Unless we have relied on another legal basis of processing, Explicit Consent is usually required for processing Sensitive Personal Data, for Automated Decision-Making and for cross-border data transfers.

5.7. We ensure that we keep records of all consents that are obtained. This is done using one of the following methods:

- copies of consent forms (electronic or in hard copy);
- a record linking the Data Subject with their consent together with the information provided to the Data Subject when consent was requested and the date on which consent was given.

6. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

6.1. As a Data Controller we provide this information to Data Subjects when Data is collected (or if it is not collected from the Data Subject within one month):

- Our organisation name and the contact details of our DPO
- The purposes of the processing and lawful basis relied upon
- Where the Personal Data was not supplied by the Data Subject: the categories of Personal Data and where it came from
- The recipient (or categories of recipients)
- The relevant retention period/s
- The Data Subject's rights
- Where applicable details of any statutory or contractual obligation to provide the Data
- Details of any automated decision making

6.2. These details are provided through appropriate Privacy Notices which will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.3. All Privacy Notices are displayed on our website and are accessible to all Data Subjects and interested parties on this link www.everest.co.uk/privacy

7. PURPOSE LIMITATION

7.1. Personal Data is collected only for specified, explicit and legitimate purposes. It is not be processed in any manner incompatible with those purposes.

7.2. Company Personnel cannot use Personal Data for new, different or incompatible purposes other than those disclosed when the Data was first obtained unless they have informed the Data Subject of the new purposes and – if their consent is required – we have obtained that consent.

8. DATA MINIMISATION

8.1. Personal Data held by us is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2. Company Personnel may only Process Personal Data when performance of their duties and responsibilities requires it.

8.3. We ensure that Personal Data collected is adequate and relevant for the intended purposes.

8.4. We ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised.

9. ACCURACY

9.1. Personal Data processed by us is accurate and, where necessary, kept up to date.

9.2. We have measures in place to ensure inaccurate data is corrected or deleted without delay.

9.3. Company Personnel take reasonable steps to ensure that the Personal Data we process is accurate, complete, kept up to date and relevant to the purpose for which we collected it.

9.4. Company Personnel check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

9.5. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. STORAGE LIMITATION

10.1. We keep Personal Data in a form which permits the identification of the Data Subject for no longer than needed for the legitimate business purpose or purposes for which we originally collected it.

10.2. Company Personnel assist us by taking reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies.

10.3. We ensure Data Subjects are informed of the period for which Data is stored and how that period is determined by issuing a suitable Privacy Notice.

11. SECURITY INTEGRITY AND CONFIDENTIALITY

11.1. Personal Data is secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

11.2. We develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks.

11.3. We regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.

11.4. Company Personnel understand their shared responsibility for protecting the Personal Data we hold. They implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. They exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

11.5. We maintain data security by protecting the confidentiality, integrity and availability of the Personal Data.

- *Confidentiality* means that only people who have a need to know and are authorised to use the Personal Data can access it
- *Integrity* means that Personal Data is accurate and suitable for the purpose for which it is processed
- *Availability* means that authorised users are able to access the Personal Data when they need it for authorised purposes

11.6. Company Personnel know they must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Laws and relevant standards to protect Personal Data.

12. REPORTING A PERSONAL DATA BREACH

12.1. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are required to do so.

12.2. If Company Personnel know or suspect that a Personal Data Breach has occurred, they do not attempt to investigate the matter themselves and know to immediately contact the office holders identified in paragraph 1.3 above.

12.3. Company Personnel know to preserve all evidence relating to any potential Personal Data Breach.

13. TRANSFER LIMITATION

13.1. We recognise that the Data Protection Laws restricts Data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the Data Protection Laws is not undermined.

13.2. Company Personnel may only transfer Personal Data outside the EEA if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks
- the transfer is necessary for one of the other reasons set out in the Data Protection Laws including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest

14. DATA SUBJECT'S RIGHTS AND REQUESTS

14.1. We recognise that Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- Withdraw Consent to processing at any time
- Receive certain information about our processing activities
- Request access to Personal Data we hold
- Prevent our use of their Personal Data for direct marketing purposes
- Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected
- Require us to rectify inaccurate Data or to complete incomplete Data
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- Object to decisions based solely on Automated Processing, including profiling and Automated Decision-Making
- Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format

14.2. We verify the identity of any individual requesting Data under any of the rights listed above and Company Personnel know not to allow third parties to persuade them into disclosing Personal Data without proper authorisation.

14.3. Company Personnel immediately forward any Data Subject request they receive to one of the office holders in paragraph 1.3 above.

15. ACCOUNTABILITY

15.1. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

15.2. We will ensure the following adequate resources and controls are in place to ensure, and to document, Data Protection Laws compliance:

- We have an appointed a Date Protection Officer and a Data Security Officer. Our Senior Managers have responsibilities that feed directly into our data compliance regime.
- We will implement Privacy by Design when processing Personal Data
- We will complete DPIAs where processing presents a high risk to rights and freedoms of Data Subjects
- We specify our approach to data protection in internal documents including this Standard and our other Polices
- We ensure Company Personnel are trained on the Data Protection Laws and maintain a record of training attendance
- We test the privacy measures implemented on a regular basis
- We conduct periodic reviews and audits to assess compliance

16. RECORD KEEPING

16.1. We will keep full and accurate records of all our data processing activities in an Information Asset Register.

16.2. All Company Personnel assist, where required, to keep and maintain accurate records.

16.3. These records will include such things as:

- The categories of Personal Data
- The categories of Data Subject
- The processing activities / purposes
- Any third-party recipients of the Personal Data,
- The storage locations
- The retention periods
- A description of the security measures in place

17. TRAINING AND AUDIT

17.1. We ensure all Company Personnel have undergone adequate training to enable them to comply with Data Protection Laws.

17.2. We must also regularly test our systems and processes to assess compliance.

17.3. We will regularly review all the systems and processes under our control to ensure they comply with this Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

18.1. We recognise that we are required to implement Privacy by Design measures when processing Personal Data. This means implementing appropriate technical and organisational measures to ensure data privacy.

18.2. We will periodically assess what Privacy by Design measures can be implemented on all programs/systems/processes by considering:

- New technologies that are available
- The cost of implementation
- The nature, scope, context and purposes of processing
- The risks to the rights and freedoms of Data Subjects posed by the processing

18.3. We will conduct DPIAs for any high-risk processing activities.

18.4. We will conduct a DPIA when implementing major system or business change programs involving the processing of Personal Data including:

- Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated processing including profiling and ADM;
- Large-scale processing of Sensitive Data;
- Large-scale, systematic monitoring of a publicly accessible area.

18.5. Our DPIAs will include:

- a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

19. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION MAKING

19.1. Automated Decision-Making is prohibited when a decision has a legal or similar significant effect on a Data Subject unless:

- a Data Subject has given explicit Consented to the processing;
- the processing is authorised by law; or
- the processing is necessary for the performance of or entering into a contract.

19.2. At present we do not undertake any Automated Processing of Personal Data, but we recognise the principles that govern such processing and will comply as and when this becomes necessary.

19.3. If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects will be informed of their right to object. This will be included in the relevant privacy notice.

19.4. We will inform the Data Subject of the logic involved in the decision making or profiling, and its significance and envisaged consequences.

19.5. We will also give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

19.6. A DPIA will be carried out before any Automated Processing (including profiling) or Automated Decision Making activities are undertaken.

20. DIRECT MARKETING

20.1. A Data Subject's prior consent is required for electronic direct marketing. However, there is a limited exception for existing customers which allows us to send marketing texts or emails in the following circumstances:

- We have obtained contact details in the course of a sale to that person
- We are marketing similar products or services
- We gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message

20.2. The right to object to direct marketing will be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

20.3. A Data Subject's objection to direct marketing will be promptly honoured.

20.4. If a Data Subject opts out at any time, their details will be suppressed as soon as possible. Suppression means retaining just enough information to ensure that marketing preferences are respected in the future.

21. SHARING PERSONAL DATA

21.1. We will not share Personal Data with third parties unless safeguards have been put in place.

21.2. We only share the Personal Data we hold with other Company Personnel, our service providers or if the recipient has a job-related need to know the information.

21.3. If sharing the Personal Data involves a cross-border transfer Company Personnel ensure they have approval to do so.

21.4. We only share Personal Data we hold with third parties, such as our service providers if:

- They have a need to know the information for the purposes of providing the contracted services
- Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained

- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place
- The transfer complies with any applicable cross border transfer restrictions
- Where required by the Data Protection Laws the Data Protection Laws processor terms are in place

22. DEFINITIONS

22.1. Please refer to the following terms which have been used in this document.

22.2. *Automated Decision-Making*: When a decision is made which is based solely on computerised algorithms, or 'Automated Processing' to produce a legal effect or significantly affect an individual, including profiling, credit decisions or matters affecting employment. The Data Protection Laws prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

22.3. *Automated Processing*: Any form of automated processing of Personal Data, and the evaluation of certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated processing

22.4. *Company Personnel*: All employees, workers, contractors, agency workers, volunteers and consultants who are engaged to work for the Company.

22.5. *Consent*: The freely-given, unambiguous indication that a Data Subject has provided a positive affirmation that they consent to particular kinds of Data being processed for particular purposes. Consent is necessary for certain special categories of sensitive Data and in order to justify the processing of Data for longer than is required under other legal bases.

22.6. *Data Breach*: An act or omission that compromises the security, confidentiality, integrity or availability of Personal Data, or a failing in the technical and organisational safeguards put in place to protect Personal Data. Any unauthorised access, disclosure, loss, damage or destruction qualifies as a Data Breach.

22.7. *Data Controller*: An organisation which holds, transfers or otherwise processes Personal Data and is in a position to make a decision about that processing.

22.8. *Data Privacy Impact Assessment* (DPIA): An assessment used to identify and reduce the risks of data processing activities. DPIAs should be undertaken to review any new major systems or activities may involving the processing of Personal Data and identify new risks and how to mitigate them. This can be carried out as part of a Privacy by Design process.

22.9. *Data Protection Laws*: Any applicable law or code of conduct which applies to the processing activities of the Company, which in the UK is the General Data Protection Regulation 2016/679 (Data Protection Laws) and the Data Protection Act 2018.

22.10. *Data Protection Officer* (DPO): A named person who leads a Company's approach to data protection. In organisations which systematically process a large quantity of Personal Data a DPO is required under the Data Protection Laws, and can be an employee or independent consultant. The DPO must report to the highest levels of governance and acts in an advisory role, while not accepting personal liability for an organisation's compliance.

22.11. *EEA*: The European Economic Area, including the 28 countries which make up the EU, and those included in the European Free Trade Agreement: Iceland, Liechtenstein and Norway.

22.12. *Data Subject*: A living identifiable individual about whom we hold Personal Data.

22.13. *Explicit Consent*: A high level of consent which requires a very clear and specific statement by the Data Subject.

22.14. *Personal Data* (or 'Data'): 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 Laws 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.

22.15. *Privacy by Design*: The process of implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the Data Protection Laws.

22.16. *Privacy Notice*: Formal written notification given to Data Subjects at the point where their Data is collected, outlining which categories of Data will be processed, the purpose for processing, retention periods and information about their rights to make requests and complaints.

22.17. *Processing or process*: Any activity that involves the use of Personal Data, including obtaining, recording, holding or carrying out any operation on the Data, such as organising, amending, retrieving, using, disclosing, erasing or destroying it. processing also includes transmitting or transferring Personal Data to third parties.

22.18. *Pseudonymised Data*: Personal Data where any information that directly or indirectly identifies an individual is replaced with one or more artificial identifiers or pseudonyms so that the individual cannot be identified without the use of additional information kept separately and securely.

22.19. *Special Categories of Sensitive Data / Sensitive Personal Data*: Specific types of protected Sensitive Personal Data, I.E.:

- Race or ethnic origin
- Political opinions
- Religious or spiritual beliefs
- Trade union membership
- Physical or mental health
- Sexual life and orientation
- Biometric or genetic Data