PRIVACY NOTICE

DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: 1. Name (including initials) 2. Identification number 3. Location data 4. Online identifier, such as a username 5. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: 1. Racial or ethnic origin 2. Political opinions 3. Religious or philosophical beliefs 4. Trade union membership 5. Genetics 6. Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes 7. Health – physical or mental 8. Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Who processes your information?
Alpine Valeting is the data controller of the personal information you provide to us. This means the company determines the purposes for which, and the manner in which, any personal data relating to clients is processed.

Ms Sarah Broadfoot, hubulu.com Ltd, 4 The Axium Centre, Dorchester Road POOLE BH16 6FE acts as a representative for the company with regard to its data controller responsibilities; they can be contacted on 07956 411172 or info@alpinevaleting.co.uk

In some cases, your data will be outsourced to a third-party processor; however, this will only be done with your consent, unless the law requires the company to share your data. Where the company outsources data to a third-party processor, the same data protection standards that Alpine Valeting upholds are imposed on the processor.

The role of the Data Protection Officer (DPO) is to oversee and monitor the company's data protection procedures, and to ensure they are compliant with the GDPR. You can also find out about the General Data Protection Regulations and Data Protection Act 2018 and your rights on the Information Commissioners Website www.ico.org.uk

Why do we collect and use your information?
Alpine Valeting holds the legal right to collect and use personal data relating to our clients and our staff. We collect such non-personal and personal information for the following purposes:

1. To provide and operate the Services;
2. To provide our Users with ongoing customer assistance and technical support;
3. To be able to contact our Visitors and Users with general or personalised service-related notices and promotional messages;
4. To create aggregated statistical data and other aggregated and/or inferred Non-personal Information, which we or our business partners may use to provide and improve our respective services;
5. To comply with any applicable laws and regulations.

We receive, collect and store any information you enter on our website or provide us in any other way. In addition, we collect the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information and purchase history. We may use software tools to measure and collect session information, including page response times, length of visits to certain pages, page interaction information, and methods used to browse away from the page.

We also collect personally identifiable information (including name, email, password, communications); payment details (including credit card information), comments, feedback, product reviews, recommendations, and personal profile.

When you conduct a transaction on our website, as part of the process, we collect personal information you give us such as your name, address and email address. Your personal information will be used for the specific reasons stated above only.

We may also receive information for staff and job applicants regarding them from their existing or previous employer/ company.

Our company is hosted on the Wix.com platform. Wix.com provides us with the online platform that allows us to sell our products and services to you. Your data may be stored through Wix.com's data storage, databases and the general Wix.com applications. They store your data on secure servers behind a firewall.

All direct payment gateways offered by Wix.com and used by our company adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of credit card information by our store and its service providers. Alpine Valeting will not share or sell your personal information with any third parties, unless the law and our policies allows us to do so.

We may contact you to notify you regarding your account, to troubleshoot problems with your account, to resolve a dispute, to collect fees or monies owed, to poll your opinions through surveys or questionnaires, to send updates about our company, or as otherwise necessary to contact you to enforce our User Agreement, applicable national laws, and any agreement we may have with you. For these purposes we may contact you via email, telephone, text messages, and postal mail.

If you don't want us to process your data anymore, please contact us at info@alpinevaleting.co.uk or send us mail to hubulu.com Ltd, 4 The Axium Centre, Dorchester Road POOLE BH16 6FE.

We reserve the right to modify this privacy policy at any time, so please review it frequently. Changes and clarifications will take effect immediately upon their posting on the website. If we make material changes to this policy, we will notify you here that it has been updated, so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we use and/or disclose it.

If you would like to: access, correct, amend or delete any personal information we have about you, you are invited to contact us at info@alpinevaleting.co.uk or send us mail to hubulu.com Ltd, 4 The Axium Centre, Dorchester Road POOLE BH16 6FE.

What are your rights?
Our clients have the following rights in relation to the processing of their personal data. You have the right to:

1. Be informed about how Alpine Valeting uses your personal data
2. Request access to the personal data that Alpine Valeting holds
3. Request that your personal data is amended if it is inaccurate or incomplete
4. Request that your personal data is erased where there is no compelling reason for its continued processing
5. Request that the processing of your data is restricted
6. Object to your personal data being processed

To make a request for your personal information, please contact our Data Protection Officer. Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way Alpine Valeting is collecting or using your personal data, you can raise a concern with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm or via the website www.ico.org.uk

APPENDIX 1

PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO). The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

1. Lost
2. Stolen
3. Destroyed
4. Altered
5. Disclosed or made available where it should not have been
6. Made available to unauthorised people

The DPO will alert the Managing Director and any client(s) affected by the breach. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure). The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

1. Loss of control over their data
2. Discrimination
3. Identify theft or fraud
4. Financial loss
5. Unauthorised reversal of pseudonymisation (for example, key-coding)
6. Damage to reputation
7. Loss of confidentiality
8. Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the company's computer system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72-hours. As required, the DPO will set out:

1. A description of the nature of the personal data breach including, where possible:
2. The categories and approximate number of individuals concerned
3. The categories and approximate number of personal data records concerned
4. The name and contact details of the DPO
5. A description of the likely consequences of the personal data breach
6. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72-hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

1. The name and contact details of the DPO
2. A description of the likely consequences of the personal data breach
3. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

1. Facts and cause
2. Effects
3. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the company's computer system. The DPO and client(s) will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

1. If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
2. Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
3. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
4. In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
5. The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
6. The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted