ZIHIPP LIMITED

DATA PROTECTION POLICY

TOPICS COVERED:

1. INTRODUCTION

This policy sets out how Zihipp Limited (the **'Company'**) handles, and how it expects its employees, staff and contractors to handle, personal data (described further below) in order to comply with our obligations under data protection legislation including the General Data Protection Regulation (EU) 2016/679 (**'GDPR'**) and the UK Data Protection Act 2018 (**'Data Protection Law'**).

The Company is committed to protecting personal data relating to our workforce, customers and other individuals that the Company holds personal data on.

All Company staff and contractors are expected to understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their work. Schedule 1 sets out the specific rules you must follow regarding the handling of personal data, including HR related personal data.

Information handling procedures cannot be reduced to a box-ticking exercise. Your obligation is to take reasonable steps to protect the rights of individuals in respect of their data and to protect people from the damage that can be caused by irresponsible data handling. This requires thought, care and most of all respect for the rights of the individual (who is referred to in the Data Protection Law as the 'data subject').

The benefits of good data practices are the protection of our brand image and improved relationships with our customers and contacts. Conversely, if our systems fall short we could be investigated by the Information Commissioner's Office ('**ICO**') which may impose substantial fines and may also publish details of its findings.

In view of the seriousness of this issue, failure to comply with this policy may lead to disciplinary action. You must also appreciate that the Data Protection Act 2018 makes it a criminal offence for any individual deliberately or recklessly to disclose or assist in the disclosure of personal data, relating to any individual (whether or not they are a client) without the Company's consent.

This policy also contains important information on how to react if a data breach occurs or is suspected. It is essential for staff to be familiar with their obligations, given the need to notify the ICO within 72 hours if a breach is suspected.

The Director of Corporate Operations is responsible for data protection compliance within the Company. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Directorate of Corporate Operations.

2. YOUR RESPONSIBILITES

The fundamental requirement of all data handling rules is that you act reasonably. You must ask yourself what you plan to do with any personal data and why, whether holding or using the information is necessary and what you can reasonably do to keep it safe.

What is Personal Data?

This policy applies to all personal data processed by the Company, and sets out the responsibility of the Company and each of our employees with respect to any personal data being processed.

'Personal data' is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data which the Company holds or is likely to obtain. This includes information:

(a) relating to job applicants, CVs and recruitment;

(b) relating to current and former staff (including employees, temporary and agency workers, interns, volunteers and apprentices) such as employment contracts, references, appraisals, medical records and immigration status;

(c) relating to third party vendors (such as payroll services and benefits providers);

(d) of customers, and of customers' employees and contractors;

(e) contained in customer data stored and/or hosted by the Company in the course of our business;

(f) how we as a business conduct marketing; and

(g) bought in or licensed from third parties.

Personal data may be held in personal computerised files (such as contacts in Microsoft Outlook) and on the Company's central document management systems. We operate various software solutions for accounting, marketing and these programs will also retain data about people. Information is also held on manual files and on paper records. Regardless of how personal data is held, Data Protection Law will apply. We remain responsible for the control of the personal data we collect even if that information is later passed on to another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by its staff).

In summary, whatever you do with information about individuals and however you do it, Data Protection Law is likely to apply.

Even where that information is a matter of public record, in many cases it is still personal data and must be treated with care and in accordance with Data Protection Law.

Processing Personal Data

'Processing' means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying personal data, or using or doing anything with it. For it to be legal for the Company to process personal data, at least one of the following conditions (known as **'lawful basis for processing'**) must be met:

(a) the data subject has consented to the processing (see below for the requirements that must be met in order to rely on consent);

(b) the processing is necessary for the performance of a contract (for example, an employment contract) to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) the processing is necessary for compliance with a legal obligation to which the Company is subject (for example, assessing a candidate's right to work in the UK);

(d) the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

(e) the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

Prior to processing personal data you must ensure that the intended processing falls into one of the above categories.

Consent to Process Personal Data

In order for consent to be valid it must be a "*freely given, specific informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

Processing Special Categories of Data

The GDPR sets out additional standards for processing special categories of data which include information relating to a data subject's: racial or ethnic origins; political opinions; religious or philosophical beliefs; trade union memberships; genetic data; biometric data; health and medical records; and sex life and sexual orientation.

These are matters that could be associated with issues of discrimination and so it follows that a data breach is more likely to cause damage. As such, the ICO demands a greater level of thought when deciding if and how you should process special category personal data.

You must only process special category data if you have **both** a lawful basis for processing as set out above under 'Processing Personal Data' **and** one of the special conditions for processing special category data set out below:

(a) The data subject has given has given their explicit consent;

(b) Processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) Processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) Processing relates to personal data which are manifestly made public by the data subject;

(e) Processing is necessary for the establishment, exercise or defence of legal claims;

(f) Processing is necessary for the purposes of preventive or occupation health and carried out under the responsibility and obligations of professional secrecy; or

(g) Processing is necessary for reasons of substantial public interest.

In respect of its employees, the Company will process the following categories of special category data:

- Health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;
- Special category data for the purposes of equal opportunities monitoring and pay equality reporting; and
- Trade union membership information for the purposes of staff administration and administering 'check off'.

Further information in respect of special category data relating to employees can be found in Schedule 1.

3. INDIVIDUAL OBLIGATIONS OF ACCURACY AND ACCESS

Individuals are responsible for helping the Company keep their personal data up to date. You should let Directorate of Corporate Operations know if the personal data you have provided to the Company changes, for example if you move house or if your bank details change.

You may have access to the personal data of other members of staff, suppliers and customers of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals.

You must:

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow other Company staff to access personal data if they have appropriate authorisation;
- Only allow individuals who are not Company staff to access personal data if you have specific authority to do so from the Directorate of Corporate Operations;

- Keep personal data secure (*eg* by complying with rules on access to premises, computer access, password protection and secure file storage and destruction);
- Not remove personal data, or devices containing personal data (or which can be used to access it), from the Company's premises unless you are authorised to do so and appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device;
- Not store personal data on local drives or on personal devices that are used for work purposes; and
- Comply with all applicable internal policies as contained in the Company's Staff Handbook and Privacy Notice and/or such other Company documentation relating to data protection from time to time.

4. DATA PROTECTION PRINCIPLES

The GDPR requires that the Company and its staff to comply with the following data protection principles when processing personal data:

(a) Personal data must be processed lawfully, fairly and in a transparent manner

In order to be transparent, the data subject must be notified of how the Company intends to use their personal data (the privacy notice) and at least one 'lawful basis for processing' must be satisfied. This will involve sending our privacy notice to those data subjects whose personal data we process.

(b) Personal data may only be collected for specified, explicit and legitimate purposes only, and must not be processed in a way that is incompatible with those legitimate purposes.

For example, if an employee or customer provides their email address for a particular issue or matter, this does not give us the right to use the email address for another purpose, such as marketing.

(c) Personal data must be adequate, relevant and necessary for the relevant purpose(s).

Any personal data that is excessive or out of date must be updated or deleted without delay.

(d) Personal data must be accurate and up to date, and reasonable steps must be taken to ensure that inaccurate personal data is deleted or corrected without delay.

(e) *Any records that the Company creates and maintains must be kept up to date, such as addresses and contact information.* **Personal data must not be kept any longer than is necessary for the purposes for which it is collected and processed.**

You are responsible for ensuring that data you use is not held longer than necessary.

(f) Personal data must be kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

You are required to ensure the security of any personal data that you process.

5. DATA PROTECTION IMPACT ASSESSMENTS ('DPIA')

Under Data Protection Law, the Company is required to consider the effect its data processing has on data privacy and to implement appropriate technical and organisation measures to minimise the risk to personal data.

Where processing is likely to result in a high risk to an individual's data protection rights (*eg* where the Company is planning to use a new form of technology which involves the capture or storage of personal data or changing a supplier that it uses for these purposes), the Company will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate in relation to its purpose;
- The risks to individuals; and
- What measures can be put in place to address those risks and protect personal data.

Before any new form of high-risk processing of personal information is introduced, the manager responsible should contact the Directorate of Corporate Operations in order that a DPIA can be carried out.

6. DOCUMENTATION AND RECORDS

As part of demonstrating compliance with Data Protection Law, the Company will keep written records of processing activities, including:

- The purposes of the processing;
- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Where possible, data retention schedules; and
- Where possible, a description of the technical and organisational security measures in place to protect the data.

Where the Company acts as a processor for a customer, the Company shall document:

- Information required for privacy notices;
- Records of consent;
- Controller-processor contracts;
- The location of personal information;
- DPIAs; and
- Records of data breaches.

7. PRIVACY NOTICE

Please see the Company's privacy notice for further details.

The Company will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The Company will conduct regular reviews of the personal information we process and update our documentation accordingly

8. SUBJECT ACCESS REQUESTS AND INDIVIDUAL RIGHTS

Under the Data Protection Laws data subjects have the right to access (*ie* to receive a copy of) the personal data we hold about them. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal information and check the lawfulness of processing to allow them to exercise their right to correct data or object to its processing, if necessary. You should be aware that this means individuals can request to see **any information that we hold about them, including copies of email and IM correspondence/documents referring to them or opinions expressed about them.**

The Company must respond to all requests for personal information within one month. Data subjects also have rights relating to the correction, erasure and restriction of processing. If you receive any requests, you must immediately notify the Directorate of Corporate Operations.

You may receive a formal request for data from a third party, purporting to have a right of access under Data Protection Law or other rule of law. No matter how official the request looks or how much it may be in the interests of the data subject to respond, you must not do so. Such requests, including court or police orders, as well as any informal looking requests must be passed to the Directorate of Corporate Operations immediately.

By law we are required to notify individuals of their rights and we do this in our privacy policies.

9. INFORMATION SECURITY

The Company will use appropriate technical and organisational measures in accordance with the Company's policies to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- Making sure that, where possible, personal data is pseudonymised or encrypted;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- Implementing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where the Company uses external organisations to process personal information on its behalf, appropriate security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- The organisation may act only on the written instructions of the Company;
- Those processing the data are subject to a duty of confidence;
- Appropriate measures are taken to ensure the security of processing;
- Sub-contractors are only engaged with the prior consent of the Company and under a written contract;
- The organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- The organisation will assist the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- The organisation will delete or return all personal information to the Company as requested at the end of the contract; and
- The organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something in breach of Data Protection Law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms from the Directorate of Corporate Operations.

10. STORAGE AND RETENTION OF PERSONAL DATA

Personal data (and special category data) will be kept securely

Personal data (and special category data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Where there is any uncertainty, staff should consult the Directorate of Corporate Operations.

Personal data (and special category data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

11. DATA BREACHES

Data Protection Law requires us to protect the personal data we hold against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data.

Despite our best efforts it is possible that data breaches will occasionally occur. A data breach may take many different forms, for example:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information either by a member of staff or a third party;
- Loss of data resulting from an equipment or systems (including hardware and software) failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as a fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.

The Company will make the required report of a data breach to the ICO without undue delay and, where possible **within 72 hours** of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

If you become aware of an actual, suspected or threatened data breach (including receiving a notification from a third party who processes personal data on the Company's behalf), you must notify the Company immediately using the details below, bearing in mind that the Company will need to react very quickly in the event of a breach:

- **During office hours, phone +44 (0)20 7459 4142 .**
- **Outside of Office Hours, phone +44 (0)20 7459 4142**

You should supply as much information about the nature and circumstances of the potential data breach and preserve all evidence relating to it.

12. INTERNATIONAL TRANSFERS

The Company may only transfer personal information to countries outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) where such countries have been designated as having an adequate level of data protection or where the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses.

Please contact the Directorate of Corporate Operations to ensure that any transfers are undertaken in a legally compliant way including any personal data to be shared with any group companies existing from time to time.

13. MARKETING

The Company is subject to certain rules and privacy laws when marketing to our customers. For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). There is a limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message. The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

14. TRAINING

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

You must undergo all mandatory data privacy-related training and (where relevant) ensure your team undergo similar mandatory training. You must regularly review any systems and processes under your control to ensure they comply with this policy

and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

15. FAILING TO COMPLY WITH THIS POLICY

The Company takes compliance with this policy (and all related policies) very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal data is being processed;
- Carries the risk of significant civil and criminal sanctions for the individual and the Company; and
- May, in some circumstances, amount to a criminal offence by the individual.

Any breach of this policy must be notified to the Directorate of Corporate Operations or, where s/he is unavailable, another member of the Legal team without delay. In particular, any unauthorised disclosure of personal data or circumstances that may lead to such disclosure must be notified immediately upon discovery.

You or others may be asked to take steps to mitigate the potential damage and such actions must be carried out promptly.

Failure to report a breach may lead to disciplinary action and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

16. REVIEW OF THIS POLICY

The Company will review and update this policy in accordance with its data protection obligations and may amend, update or supplement it from time to time. The Company will circulate any new or modified policy to staff when it is adopted.

SCHEDULE 1

RULES AND PROCEDURES FOR THE HANDLING OF PERSONAL DATA

KEY CONSIDERATIONS FOR HANDLING ANY PERSONAL DATA

Before you begin a new activity that involves processing personal data consider the following:

- Do you need to record/collect/share the personal data? Could the same objective be achieved without processing personal data? Could anonymised (or pseudonymised) data be used instead?
- Do you have a lawful basis for processing the data (for example, is it required for performance of a contract or necessary to comply with a legal obligation)? Is the purpose for which you are processing the personal data covered by our privacy policy? If not, have you informed the Directorate of Corporate Operations so that our register of data processing activities can be updated?
- Has the data subject been told about the processing (i.e. have they received a copy of our privacy policy)?
- Are you authorised to process the personal data? For example, if you are processing personal data for direct marketing or processing special categories of personal data in circumstances where litigation is not contemplated and the consent of the data subject is required, has this been obtained and documented?
- Have you checked that the personal data is accurate?
- Are you confident that the personal data will be secure throughout the processing?
- Do you plan to pass the data on to a third party or transfer it outside the UK? If so, is the Directorate of Corporate Operations aware of the data sharing? Do we have the necessary contracts and permissions in place to do this?
- Are you setting up new procedures or systems that involve personal data (for example new databases for storing personal data or data sharing initiative)? If so, have you complied with the Data Protection Impact Assessment guidelines?

When going about handing personal data, consider the following practical steps:

- When sending out correspondence, such as emails and letters, addresses must be correct and applied with particular care. If correspondence is sensitive, consider if encryption or recorded delivery is appropriate.
- Where emails include personal data, your computer must be locked when unattended.
- Hard copy documents containing personal data should not be left unattended and should be locked away overnight.
- Documents containing personal data must not be left on the photocopier or any other work surfaces.
- Where documents are in your care away from office premises, you must ensure they are safe from fire, flood, theft or other perils that could lead to destruction.

- Where documents containing personal data are to be destroyed, they must be placed in the shredding facilities and not the general refuse. If in doubt, always use the shredding bins or confidential waste bins.
- When discussing personal data away from the office (face to face or by telephone) you must take care that you are not overheard by members of the public.
- Documents must not be removed from the office unless absolutely necessary and must only be removed for the period they are required. As soon as you no longer need them, they must be returned.
- When carrying documents on public transport or in public places, ensure the documents remain with you at all times. Stowing documents away (for example in the overhead compartments on a train or under a restaurant table) will increase the likelihood of you forgetting to take them with you.
- Documents must not be left in unattended cars or unattended bags/cases, no matter how secure that car or case may be.
- When storing documents at home, they must be protected from the view of visitors.

ADDITIONAL CONSIDERATIONS FOR HANDLING PERSONAL DATA OF COMPANY PERSONNEL

The Company will hold personal information about its employees, consultants, contractors and the staff of its contractors (**'Personnel'**) which may include but not be limited to the following (**'Personnel Information'**):identification documents, such as passports and driving licenses; contact details, including home addresses; employment history, qualifications and skills; employment contracts; references; immigration and visa details; national insurance numbers; trade union memberships; appraisals, absence records, disciplinary records and grievance records; health and medical information; and salary and benefit details.

Any personal information relating to Personnel is to be treated as Personnel Information and constitutes personal data as defined under Data Protection Law.

Personnel are data subjects and Personnel Information must be handled in accordance with Data Protection Law. The majority of Personnel Information is gathered, stored and processed by HR, however, most people working at the Company will handle Personnel Information of some sort on some occasions.

Whilst it is often appropriate to allow employee data to pass between various departments within the Company, Personnel Information must reach only those individuals who have a legitimate reason to receive it. For this reason, in addition to meeting the general obligations as set out in this Policy, you are also expected to comply **with the following additional rules when handling Personnel Information** (and it is best practice to also follow these additional rules when handling all types of personal data):

- **Labelling of Personal Data**
    - When sending an email containing Personnel Information you should categorise it as "**private**" or "**confidential**" using your email tags or by clearly stating so in the subject of the email.

- Where Personnel Information is to be sent by hard copy document between offices or externally, it should be secured in a sealed envelope clearly marked "**Private and Confidential**".

- **Disclosure of Personnel Information**
    - Personnel Information should not be divulged to other Personnel or external third parties unless you have the subject's consent. For example, you should not release a colleague's address or home telephone number without their consent.

When answering a call for Personnel who are on holiday or sick, it is acceptable to say they are not in the office and, if necessary, how long they will be away for. You should not disclose their reason for absence unless you have their consent. For example, any medical or sickness information should not be revealed when explaining absences.