DATA PROTECTION POLICY - Huboo Technologies Limited
("Huboo", "we", "us", "our")

1 Purpose and scope of this policy

1.1 You'll be familiar with how personal data is processed by commercial organisations from your visits to websites (cookie consents anyone?) and any forms you complete acknowledging how your personal details will be used. Those organisations make you aware in this way to ensure their compliance with relevant law.

1.2 Huboo is no different in having to comply with the law. We recognise that the correct and lawful treatment of personal data will maintain confidence in Huboo and will provide a sound basis for appropriate and successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times and in turn we expect all our people to do the same. As a result, we seek to minimise the risk to individuals from processing their personal data. Failing to do that can result in breach of legislation, reputational damage, or financial implications due to fines.

1.3 We are exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher, for failure to comply with applicable law. In the UK, that law is contained in the UK version of the EU's General Data Protection Regulation and the Data Protection Act 2018. In the EU countries where we operate, the EU's General Data Protection Regulation applies. The legal obligations which apply to us are described as "applicable law" in this policy.

1.4 This policy is part of demonstrating that we have appropriate measures and records in place to show that that we take responsibility for what we do with personal data in compliance with applicable law.

1.5 This policy provides important information about:

(a) what is meant by personal data, sensitive personal data and other related terms (**section 1** of the **Appendix**);
(b) the data protection principles that Huboo must comply with (**section 2**);
(c) the lawful bases on which we are permitted to process personal data (**section 3**);
(d) specific important requirements for processing sensitive personal information (**sections 4 and** 5);
(e) requirements for carrying out data protection assessments and keeping adequate records (**sections 6 and 7**);
(f) where more detailed information can be found about the personal data we gather and use about everyone who works for Huboo and external people who interact with or use huboo (**section 8**);
(g) rights and obligations in relation to data protection (**sections 9 and 10**);
(h) information security arrangements we must have in place (**section 11**);
(i) how we store and retain personal data (**section 12**);
(j) breaches of data protection requirements (**section 13**);
(k) transferring personal data internationally (**section 14**); and
(l) the consequences of failure to comply with this policy (**section 16**).

1.6 This policy applies to all personal data we process regardless of the media on which data are stored or whether it relates to past or present employees, workers, customers (and their customers), clients or supplier contacts, shareholders, website users or any other data subject.

1.7 This policy applies to all employees, workers, agency workers, independent contractors, freelancers, volunteers or interns ("you", "your"). You must read, understand and comply with this policy so that you understand what is expected of you if you process any personal data on our behalf. You must also attend

any training we run on its requirements. This policy sets out what we expect from you in order for Huboo to comply with applicable law.

1.8 We will make available related policies and guidelines to help you interpret and act in accordance with this policy. You must also read, understand and comply with all such related policies and guidelines. Any breach of this policy or related policies and guidelines may result in disciplinary action.

1.9 Where you have a specific responsibility in connection with personal data processing such as capturing consent to use a third party's personal data, reporting a personal data breach, conducting a data protection impact assessment (DPIA) or otherwise then you must comply with the related policies and guidelines.

1.10 This policy and all related policies and guidelines are internal documents and cannot be shared with anyone outside Huboo without prior authorisation from our Data Protection Officer (DPO), [redacted]. If you have any questions about this policy, please contact our DPO. Our DPO is responsible for informing and advising Huboo and its staff on its data protection obligations, and for monitoring compliance with those obligations and with Huboo's policies.

1.11 This policy has been shared with you via our HR System called Bob. Once you have read and understood this policy, please confirm that you have done so by signing this document via Bob. By signing you confirm that you have read and understood this policy and agree to abide by its terms.

1.12 We will review and update this policy periodically in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

You'd expect any company processing your personal data (including their employees) to take care of your data and meet their legal obligations. For the same reason, everyone in Huboo is expected to understand our (and their) obligations relating to data protection. We've set the detail out in the Appendix. It's important that you read and understand this.

APPENDIX

1 Definitions

We've included definitions of certain terms below to help with your understanding of this policy:

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
data subject	means the individual to whom personal data relates (this can be an employee or other staff member, an end customer where we are fulfilling an order with our client, or a client or supplier contact);
personal data	(sometimes known as personal information or personally identifiable information or PII) means information relating to an individual who can be identified (directly or indirectly) from that information. This could be personal data relating of a member of staff at Huboo or a contact at a customer or the recipient of an order that we are fulfilling for a customer;
processing	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymisation	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data', 'special category data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

2 Data protection principles

Huboo will comply with the following data protection principles when processing personal data:

2.1 we will process personal data lawfully, fairly and in a transparent manner;
2.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process such data in a way that is incompatible with those legitimate purposes;
2.3 we will only process personal data to the extent that such processing is adequate, relevant and necessary for the relevant purposes;
2.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;
2.5 we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed;

2.6 we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

2.7 we will not transfer personal data to another country without appropriate safeguards being in place;

2.8 we will allow data subjects to exercise certain rights in relation to their personal data;

2.9 we will be responsible for and must be able to demonstrate compliance with the data protection principles listed above.

3 Basis for processing personal information

3.1 We're only permitted to collect, process and share personal data fairly, lawfully in a transparent manner in relation to each data subject, and for specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process fairly and without adversely affecting the data subject.

3.2 Applicable law allows processing for specific purposes which reflect certain lawful bases on which we can process personal data, including where:

(a) the data subject has consented to the processing;
(b) the processing is necessary for the performance of a contract between Huboo and the data subject 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 Huboo is subject;
(d) the processing is necessary for the protection of the vital interests of the data subject or another person; or
(e) the processing is necessary for the purposes of our legitimate interests or those of a third party, except where those interests are outweighed by the interests of fundamental rights and freedoms of the data subject.

3.3 These requirements mean that we must take certain steps in how we process personal data:

(a) except where the processing is based on consent from a data subject, we must satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);
(b) we must document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
(c) we must include information about both the purposes of any processing and the lawful basis for it in our relevant privacy notice(s);
(d) where sensitive personal information is processed, we must also identify a lawful special condition for processing that information (see paragraph 4.1(b) below), and document it; and
(e) where criminal offence information is processed, we must also identify a lawful condition for processing that information, and document it.

3.4 If we believe that Huboo's (or a third party's) legitimate interests are the most appropriate basis for lawful processing, we will:

(a) conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision (an example is our CCTV policy under which we process personal data contained in CCTV images and to be compliant, we have carried out an LIA in relation to our processing);
(b) if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
(c) keep the LIA under review, and repeat it if circumstances change; and
(d) include information about our legitimate interests in our relevant privacy notice(s).

4 Sensitive personal information

4.1 Huboo may from time to time process sensitive personal information. Typically, this will only occur in relation to our staff, but it might also occur if we fulfil products for a customer that reveal any of the special categories within the meaning of sensitive personal information about an end customer. We will only process sensitive personal information if:

(a) we have a lawful basis for doing so as set out in paragraph 3.2 above, eg it is necessary for the performance of the employment contract, to comply with Huboo's legal obligations or for the purposes of Huboo's legitimate interests; and
(b) one of the special conditions for processing sensitive personal information applies, eg:
- the data subject has given us explicit consent (whether directly or indirectly);
- the processing is necessary for the purposes of exercising the employment law rights or obligations of Huboo or the data subject;
- the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
- processing relates to personal data which are manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims; or
- the processing is necessary for reasons of substantial public interest.

4.2 If we are processing any sensitive personal information of a type that we have not processed previously, staff must notify our DPO of the proposed processing, so that he may assess whether the processing complies with the criteria noted above.

4.3 Sensitive personal information will not be processed until:

(a) the assessment referred to in paragraph 4.2 has taken place; and
(b) the individual (data subject) has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

4.4 Huboo will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

4.5 Huboo's Data protection privacy notice (all staff) sets out the types of sensitive personal information that Huboo processes, what it is used for and the lawful basis for the processing.

4.6 In relation to sensitive personal information relating to our staff, Huboo will comply with the procedures set out in paragraphs 4.7 and 4.8 below to make sure that our processing complies with the data protection principles set out in section 2 above.

4.7 **During the recruitment process**: the HR department, with guidance from our DPO, will ensure that (except where the law permits a different approach):

(a) during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, eg race or ethnic origin, trade union membership or health;
(b) if sensitive personal information is received, eg the applicant provides it without being asked for it within their CV or during the interview, we will delete or redact it and pending such steps, it will be disregarded and used only to the extent that such use is essential for the purpose received;

(c) any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;
(d) 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;
(e) we will not ask health questions in connection with recruitment other than as necessary to ensure that applicants are aware of and comfortable with the requirements of a role.

4.8 **During employment**: the HR department, with guidance from our DPO, will process:

(a) health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;
(b) sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting; and
(c) trade union membership information for the purposes of staff administration and administering 'check off'.

In relation to processing of personal data relating to our staff (whether sensitive or not), please refer to our Data protection privacy notice (all staff).

5 Criminal records information

Criminal records information will be processed for the purposes of ensuring that we safeguard our employees, customers, suppliers and business interests.

6 Data protection impact assessments (DPIAs)

6.1 Where processing is likely to result in a high risk to an individual's data protection rights (eg where Huboo is planning to use a new form of technology that processes personal data), we will, before commencing the processing, carry out a DPIA to assess:

(a) whether the processing is necessary and proportionate in relation to its purpose;
(b) the risks to individuals; and
(c) what measures can be put in place to address those risks and protect personal information.

We will develop a process under which you will be expected to carry out your own DPIA if required but in the meantime, if you believe one is required, please contact our DPO.

7 Documentation and records

7.1 We will:

(a) keep written records of processing activities;
(b) conduct periodic reviews of personal information we process and update our documentation accordingly; and
(c) document our processing activities in electronic form so we can add, remove and amend information easily.

8 Privacy notice and policy

8.1 Huboo will issue a privacy notice to you from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

8.2 We also have a website privacy policy (Privacy Notice | Huboo) and cookies notice (Cookies Notice | Huboo) which provide information to anyone externally using huboo.com or our services, or anyone whose personal data we may process (eg end customers of our customers) about how we process their data.

9 Individual rights

9.1 You (in common with other data subjects) have the following rights in relation to your personal information:

(a) to be informed about how, why and on what basis that information is processed — see Huboo's Data protection privacy notice (all staff);
(b) to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request;
(c) to have data corrected if it is inaccurate or incomplete;
(d) to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
(e) to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where Huboo no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
(f) to restrict the processing of personal information temporarily where you do not think it is accurate (and Huboo is verifying whether it is accurate), or where you have objected to the processing (and Huboo is considering whether our legitimate grounds override your interests).

9.2 If you wish to exercise any of the rights in paragraphs (a) to (f) above, please contact our HR team inbox [redacted].

10 Individual obligations

10.1 You are responsible for helping us keep your personal information up to date. You should let the HR team know [redacted] if the information you have provided to Huboo changes, for example an address or bank account change. Alternatively, you can update your own personal information on a secure basis via Huboo's HR information system.

10.2 You may have access to the personal information of other members of staff, Huboo's suppliers, clients or their customers in the course of your employment or engagement. If so, Huboo expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 9.1 above. Such personal information is confidential and you must also comply with the obligations of confidentiality contained in your employment contract.

10.3 If you have access to personal information, you must:

(a) only access the personal information that you have authority to access, and only for authorised purposes;
(b) only allow other Huboo staff to access personal information if they have appropriate authorisation;

(c) only allow individuals who are not Huboo staff to access personal information if you have specific authority to do so from your business area director and all other internal approval processes have been followed;
(d) keep personal information secure (eg by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in Huboo's information security policy which can be found at [redacted] or which are developed under that policy and shared with you in future);
(e) not remove personal information, or devices containing personal information (or which can be used to access it), from Huboo's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
(f) not store personal information on local drives or on personal devices that are used for work purposes.

10.4 You should contact our Data Protection Officer [redacted] if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

(a) processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 4.1(b) being met;
(b) any data breach as set out in paragraph 13.1 below;
(c) access to personal information without the proper authorisation;
(d) personal information not kept or deleted securely;
(e) removal of personal information, or devices containing personal information (or which can be used to access it), from Huboo's premises without appropriate security measures being in place;
(f) any other breach of this policy or of any of the data protection principles set out in paragraph 3 above.

11 Information security

11.1 Huboo will use appropriate technical and organisational measures in accordance with Huboo's Information Security policy (see link above) to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. This relies on you meeting your individual obligations relating to the protection of personal and confidential information (see section 10 above).

11.2 Where Huboo uses external organisations to process personal information on its behalf, additional 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:

(a) the organisation may act only on the written instructions of Huboo;
(b) those processing the data are subject to a duty of confidence;
(c) appropriate measures are taken to ensure the security of processing;
(d) sub-contractors are only engaged with the prior consent of Huboo and under a written contract;
(e) the organisation will assist Huboo in providing subject access and allowing individuals to exercise their rights in relation to data protection;
(f) the organisation will assist Huboo in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
(g) the organisation will delete or return all personal information to Huboo as requested at the end of the contract; and
(h) the organisation will submit to audits and inspections, provide Huboo with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Huboo immediately if it is asked to do something infringing data protection law.

11.3 Before any new contract involving the processing of personal information by an external organisation is entered into, or an existing contract is altered, the relevant staff must seek approval of its terms by our DPO.

12 Storage and retention of personal information

12.1 Personal information (and sensitive personal information) will be kept securely in accordance with Huboo's Information Security policy.

12.2 Personal information (and sensitive personal information) 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. We are working to complete a Data Retention policy which will contain more information about the retention periods that apply to various data and documents that we create and use. We will provide more information on this, update this policy and include a link to the new policy in due course.

12.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

13 Data breaches

13.1 A data breach may take many different forms, for example:

(a) loss or theft of data or equipment on which personal information is stored;
(b) unauthorised access to or use of personal information either by a member of staff or third party;
(c) loss of data resulting from an equipment or systems (including hardware and software) failure;
(d) human error, such as accidental deletion or alteration of data;
(e) deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
(f) 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

13.2 Huboo will:

(a) report any data breach to the Information Commissioner's Office 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 affected individuals; and
(b) 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.

14 International transfers

14.1 Huboo will only transfer personal information outside the UK to one of its overseas locations and/or to international organisations on the basis that that country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards. If not, Huboo will use other safeguards.

15 Training

15.1 Huboo will ensure that staff are adequately trained regarding their data protection responsibilities including appropriate training where roles require regular access to personal information or are responsible for implementing this policy or responding to subject access requests under this policy.

16 Consequences of failing to comply

16.1 Huboo takes compliance with this policy very seriously. Failure to comply with the policy:

(a) puts at risk the individuals whose personal information is being processed; and
(b) carries the risk of significant civil and criminal sanctions for the individual and Huboo; and
(c) may, in some circumstances, amount to a criminal offence by the individual.

16.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, 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.

16.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact our Data Protection Officer [redacted].

I have read and understood this policy and agree to abide by its terms.

Signed.....Date…….