Lucra Personal Data Protection Policy

1 Policy statement

1.1 This Data Protection Policy ("Policy") sets out how the Lucra Group ("**Lucra**", "**we**", "**us**", "**our**") handles Personal Data. The key definitions used in this Policy are set out in paragraph 3.

1.2 This Policy applies to all Personal Data that we Process regardless of the media on which that Personal Data is stored or whether it relates to past or present customers, clients of our customers, third parties involved in transactions that we facilitate, employees, workers, supplier contacts, shareholders, website users or any other Data Subject.

1.3 Everyone has rights in relation to how their Personal Data is handled. We recognise that the correct and lawful treatment of Personal Data will maintain confidence in Lucra as a business.

1.4 Applicable legislation imposes significant fines for failing to lawfully Process and safeguard Personal Data and failure to comply with this Policy may result in those fines being applied.

1.5 Lucra Personnel are obliged to comply with this Policy when Processing Personal Data on our behalf. Any breach of this Policy may result in disciplinary action.

2 About this Policy

2.1 This Policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, transfer, store or otherwise Process Personal Data.

2.2 This Policy does not form part of any employee's contract of employment and may be amended at any time.

2.3 Our DPO is responsible for ensuring compliance with Data Protection Legislation and with this Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to our DPO.

2.4 This Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3 Definition of data protection terms

3.1 In this policy, we use the following defined terms:

"**Controller**" means any person or organisation who determines the purposes for which, and the manner in which, any Personal Data is Processed. The Controller is responsible for establishing practices and policies in line with Data Protection Legislation.

"**Data Protection Legislation**" means all applicable data protection and privacy legislation including the United Kingdom General Data Protection Regulation (as defined in section 3(10) and supplemented by section 205(4)) of the Data Protection Act 2018) (the "UK GDPR"), the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 ("EU GDPR") and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

"**DPO**" means Data Protection Officer. We have appointed Peter Davey as our DPO. You can contact Peter at info@lucra.cc.

"**Data Subjects**" for the purpose of this Policy means all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

"ICO" means the Information Commissioner's Office, the supervisory authority for data protection in the UK.

"Lucra Group" means Vandelay Holdings Limited and its subsidiaries including Lucra Technologies Limited (which is wholly owned by Vandelay Holdings Limited).

"Lucra Personnel" means all employees, workers, contractors, consultants, directors and members of Lucra. Lucra Personnel must protect the Personal Data that they handle in accordance with this Policy and any applicable Personal Data security procedures at all times.

"Personal Data" means any information relating to an identified or identifiable living, natural person (a Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Privacy by Design" means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the Data Protection Legislation.

"Processing" is any activity that involves use of Personal Data. It includes obtaining, recording or holding Personal Data, or carrying out any operation or set of operations on Personal Data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties. 'Process' and 'Processed' will be interpreted accordingly.

"Processors" means any person or organisation that is not Lucra Personnel that processes Personal Data on our behalf and on our instructions, such as suppliers that handle Personal Data on behalf of Lucra (for example, our cloud hosting provider).

"Special Category Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4 Data protection principles

4.1 Any Processing of Personal Data must comply with the six data protection principles. These provide that Personal Data must be:

(a) Processed fairly and lawfully and transparently in relation to the Data Subject ("**Lawfulness, Fairness and Transparency**") – see paragraphs 5 and 6;

(b) collected only for specified, explicit and legitimate purposes and not further Processed in a way that is incompatible with the original purpose(s) for which it was collected ("**Purpose Limitation**") – see paragraph 7;

(c) adequate, relevant and limited to what is necessary for the purpose(s) for which it is collected ("**Data Minimisation**") – see paragraph 8;

(d) accurate and up to date ("**Accuracy**") – see paragraph 9;

(e) not kept longer than necessary for the purpose(s) for which it was collected ("**Storage Limitation**") – see paragraph 10; and

(f) Processed securely using appropriate technical and organisational measures ("**Security**") – see paragraph 11.

4.2 We are responsible for and must be able to demonstrate compliance with the six data protection principles listed at paragraph 4.1 above.

5 Lawfulness and Fairness

5.1 Data Protection Legislation is not intended to prevent the Processing of Personal Data, but to ensure that such Processing is done fairly and without adversely affecting the rights of the Data Subject.

5.2 For Personal Data to be processed lawfully, it must be processed on the basis of one of the lawful bases set out in the Data Protection Legislation and not otherwise contravene applicable law and regulatory guidance. Where we act as a Controller, one of the below lawful bases must apply in respect of each purpose for which we Process Personal Data:

(a) Processing is necessary for the performance of a contract between the Data Subject and Lucra, or in order to take steps to enter into such a contract at the request of the Data Subject;

(b) Processing is necessary to comply with a legal obligation to which we are subject;

(c) Processing is necessary to protect the vital interests (physical integrity or life) of the Data Subject or others;

(d) Processing is necessary for the purposes of the legitimate interests pursued by Lucra or another Controller except where those interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child; or

(e) Data Subject has consented to the Processing for the specific purposes the Personal Data is to be processed for (such consent to be a freely given, specific, informed, unambiguous indication made by a statement or clear affirmative action signifying agreement).

5.3 Special Category Personal Data is Personal Data which is deemed more sensitive and therefore afforded additional protection under the Data Protection Legislation. In order to Process Special Category Personal Data, we must ensure that we have a lawful basis, as well as an additional "condition". The conditions most likely to be applicable to Lucra include:

(a) Processing is necessary for Lucra to carry out its obligations and exercise its rights, or the rights of individuals, in the fields of employment, social security and social protection law;

(b) Data Subject has given explicit consent to the Processing for the specific purposes Data is to be processed for (such consent to be a freely given, specific, informed, unambiguous indication made by a statement or clear affirmative action signifying agreement); or

(c) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

5.4 Other conditions may be available for Processing Special Category Personal Data. Contact the DPO for more information.

5.5 Where Personal Data relating to criminal convictions is being Processed, this shall only be done where authorised by law or under the control of official authority.

6 Transparency

6.1 We will be open and transparent about how we Process Personal Data. We will inform Data Subjects about how and why we Process their Personal Data by providing appropriate notices to such Data Subjects, including by way of our privacy policies. This will include the following information:

(a) our identity and contact details and the contact details of our DPO;

(b) the purpose or purposes and lawful bases for which we intend to Process that Personal Data, and the specific legitimate interest relied upon if that is the lawful basis for Processing;

(c) the types of third parties, if any, with which we will share or to which we will disclose that Personal Data;

(d) whether the Personal Data will be transferred outside the UK and/or European Economic Area ("**EEA**") (as applicable) and if so the safeguards in place;

(e) the period for which their Personal Data will be stored or the criteria used to determine the period of retention;

(f) the existence of any automated decision making in the Processing of the Personal Data along with the significance and envisaged consequences of the Processing; and

(g) the rights of the Data Subject to limit Processing, request information, request deletion of information or lodge a complaint with a supervisory authority such as the ICO.

6.2 If we receive Personal Data about a Data Subject from other sources, we will provide the Data Subject with this information in advance or as soon as possible thereafter.

7 Purpose Limitation

7.1 In the course of our business, we will collect and Process Personal Data. This may include Personal Data we receive directly from a Data Subject (for example, when a Data Subject creates an account or corresponds with us on the Lucra platform, by phone, email or otherwise) and Personal Data we receive from other sources (including, for example, law firm customers, sub-contractors in technical, payment and delivery services and others).

7.2 We will only process Personal Data for the specific purposes notified to the Data Subject when the Personal Data was first collected or for any other purposes specifically permitted by the Data Protection Legislation. This means that Personal Data must not be collected for one purpose and then used for another purpose which is incompatible with the purpose for which it was collected.

8 Data Minimisation

8.1 We will only collect Personal Data to the extent that it is required for the specific purposes for which we collect it.

8.2 We will implement measures to ensure that we are collecting the minimum amount of Personal Data necessary to fulfil our intended purposes, for example, by ensuring that our Lucra platform

account sign up page does not request Personal Data which is not required for us to provide our services.

9 Accuracy

We will ensure that Personal Data that we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10 Storage Limitation

We will not keep Personal Data in a form which permits identification of Data Subjects for longer than is necessary for the purpose(s) for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all Personal Data which is no longer required.

11 Security

11.1 We will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

11.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves. Contracts with Processors will comply with Data Protection Legislation and contain explicit obligations on the Processor as required under the Data Protection Legislation.

11.3 We will maintain Personal Data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the Personal Data if they need it for authorised purposes. Personal Data should therefore be stored on Lucra's central computer system instead of individual devices.

11.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Access controls.** Electronic files containing Personal Data should be accessible only by those with a business need to access that information.

(c) **Password protection.** Electronic files containing particularly sensitive Personal Data should be password protected.

(d) **Use of network.** Electronic files containing Personal Data should not be stored on Lucra Personnel personal drives or desktops, and should instead be stored on the network.

(e) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal Data is always considered confidential.)

(f) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. Personal Data stored electronically by Processors on Lucra's behalf (such as cloud service providers) should be irreversibly deleted.

(g) **Equipment.** Lucra Personnel must ensure that individual screens do not show confidential information to passers-by and that they log off from their devices when they are left unattended.

(h) **Encryption.** Devices and equipment should be encrypted.

12 Processing in line with Data Subjects' rights

12.1 We will process all Personal Data in line with Data Subjects' rights, in particular their right to:

(a) withdraw consent to Processing at any time;

(b) receive certain information about our Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA and/or UK (as applicable);

(i) object to decisions based solely on automated Processing, including profiling;

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) 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.

13 Dealing with Data Subject Requests

13.1 Data Subjects may contact us to exercise their rights under the Data Protection Legislation in relation to the Personal Data that we hold about them ("**Rights Request**"). Rights Requests can be made in any form including orally and in writing (email or post). Lucra Personnel who receive a Rights Request should forward it to the DPO immediately.

13.2 We will verify the identity of an individual requesting data under any of the rights listed in paragraph 12 (Lucra Personnel must not allow third parties to persuade them into disclosing Personal Data without proper authorisation).

13.3 Personal Data relating to individuals other than the person who has made the Rights Request shall not be disclosed unless those other individuals have consented to the disclosure or it is reasonable in all the circumstances to disclose the information. Advice should be sought from the DPO on disclosure of third party Personal Data.

13.4 A Rights Request must be dealt with and a response provided to the Data Subject without undue delay and at the latest within one month of receipt of the request. We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. Where we propose to extend time, we must let the individual know within one month of receiving their request and explain why the extension is necessary.

13.5 Subject to 13.6, no fee shall be charged for the Rights Request.

13.6 If the Rights Request is manifestly unfounded, excessive or is a request for additional copies of the same information then a reasonable fee may be charged based on the administrative cost of providing the information.

14 Privacy by Design and Data Protection Impact Assessments

14.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data protection principles (set out in paragraph 4 above).

14.2 Lucra Personnel must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

14.3 Controllers must conduct and record a Data Protection Impact Assessment ('DPIA') in respect of the Processing of Personal Data which poses a high risk for Data Subjects.

14.4 Lucra Personnel should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) automated Processing including profiling and automated decision making;

(c) large-scale Processing of Special Category Personal Data or criminal convictions Personal Data; and

(d) large-scale, systematic monitoring of a publicly accessible area.

14.5 A DPIA must include:

(a) a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

14.6 We have a standard form DPIA which can be found here. All DPIAs require approval from the DPO.

14.7 Where the lawful basis of legitimate interests is relied upon, a legitimate interest assessment ('LIA') must be completed and recorded. The LIA must cover the following three tests:

(a) Purpose test: are you pursuing a legitimate interest?

(b) Necessity test: is the processing necessary for that purpose?

(c) Balancing test: do the individual's interests override the legitimate interest?

14.8 We have a standard form LIA which can be found here. All LIAs require approval from the DPO.

15 Transferring Personal Data to a country outside the UK or the EEA

Transfers of Personal Data outside the UK and the EEA are restricted under the UK GDPR and the EU GDPR respectively. We will only transfer Personal Data outside the UK and/or the EEA, as applicable, in the following circumstances:

(a) the country to which the Personal Data is being transferred has been deemed to provide an adequate level of protection by the UK Government and/or the European Commission, as applicable;

(b) we have put in place standard contractual clauses which are approved by the Information Commissioner's Office or the UK Government and/or the European Commission, as applicable, with the third party to whom we are transferring the Personal Data, provided that we have also determined that the country to which the Personal Data will be transferred provides an essentially equivalent level of protection for the Personal Data as it would have in the UK and/or the EEA, as applicable; or

(c) a derogation applies under the UK GDPR and/or the EU GDPR, as applicable.

16 Disclosure and sharing of personal information

16.1 We may share Personal Data that we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries.

16.2 We may also disclose Personal Data we hold to third parties:

(a) in the event that we sell or buy any business or assets, or any part of our business or assets, in which case we may disclose Personal Data that we hold to the prospective seller or buyer of such business or assets;

(b) if we or substantially all of our assets are acquired by a third party, in which case Personal Data that we hold will be one of the transferred assets;

(c) in connection with the services that we provide and otherwise in connection with the effective running of our business;

(d) if we are under a duty to disclose or share Personal Data in order to comply with any legal obligation;

(e) in order to enforce or apply any contract with the Data Subject or other agreements; or

(f) to protect our rights, property, or the safety of Lucra Personnel or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

16.3 We may also share Personal Data we hold with third parties, identified by name or category, for the purposes made clear to the Data Subject within our privacy policies.

17 Personal Data Breaches

17.1 Failing to appropriately deal with and report a Personal Data Breach can have serious consequences for Lucra and for Data Subjects including:

(a) risk to the Data Subjects including identity fraud, financial loss, distress or physical harm;

(b) reputational damage to Lucra;

(c) fines imposed under the UK GDPR of up to the higher of £17.5 million or 4% of global annual turnover; and/or

(d) fines imposed under the EU GDPR of up to the higher of €20 million or 4 % of annual global turnover.

17.2 A Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A Personal Data Breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential Personal Data Breaches are listed below:

(a) leaving a mobile device on a train;

(b) theft of a bag containing paper documents;

(c) destruction of the only copy of a document; and

(d) sending an email or attachment to the wrong recipient.

18 Reporting a Personal Data Breach

18.1 If you suspect a Personal Data Breach may have occurred then you must contact the DPO immediately at info@lucra.cc.

18.2 If a notification to a supervisory authority such as the ICO is required by law in relation to the Personal Data Breach then notification must be made within 72 hours of discovery of the Personal Data Breach where we are a Controller of the compromised Personal Data. It is therefore important that all potential Personal Data Breaches are reported internally to the DPO immediately. Lucra Personnel who fail to report a potential Personal Data Breach could face disciplinary action.

19 Investigating a Personal Data Breach

19.1 The DPO will assess each report of a potential Personal Data Breach and take the following steps:

(a) Breach minimisation: Liaise with IT to take steps where appropriate to minimise the impact of the Personal Data Breach. Appropriate measures may include:

(i) remote deactivation of mobile devices;

(ii) shutting down IT systems; and

(iii) recovering lost data.

(b) Breach investigation: Investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

(i) what data/systems were accessed;

(ii) how the access occurred;

(iii) how to fix vulnerabilities in the compromised processes or systems; and

(iv) how to address failings in controls or processes.

(c) Breach analysis: Analyse the Personal Data Breach to determine:

(i) how many data subjects were affected;

(ii) what data was accessed, and whether it was special category data; and

(iii) what notifications are required (see 'External Communication' below).

20 External communication

20.1 All external communication is to be managed and overseen by the DPO.

20.2 **Law Enforcement.** The DPO will assess whether the Personal Data Breach incident requires reporting to the Police e.g. if it involved theft. The DPO shall coordinate communications with the Police and the collection of internal reports and evidence where appropriate.

20.3 **ICO or other supervisory authority notification.** If Lucra is the Controller in relation to the Personal Data involved in the Personal Data Breach then we will have 72 hours to notify an appropriate supervisory authority(ies) if the breach is notifiable. A Personal Data Breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of individuals. The DPO will make an assessment of the Personal Data Breach against this criteria taking into account the facts and circumstances in each instance, taking into account:

(a) the type and volume of Personal Data involved in the Personal Data Breach;

(b) whether any Special Category Data was involved;

(c) the likelihood of the Personal Data being accessed by unauthorised third parties;

(d) the security in place in relation to the Personal Data, including whether it was encrypted; and

(e) the risks of damage or distress to the Data Subject.

If a notification to a supervisory authority is required, then a report to the relevant supervisory authority should be prepared.

20.4 **Data Subjects.** When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subjects then the Data Subject must be notified without undue delay. The communication will be coordinated by the DPO and will include at least the following information:

(a) a description in clear and plain language of the nature of the Personal Data Breach;

(b) the name and contact details of the DPO;

(c) the likely consequences of the Personal Data Breach;

(d) the measures taken or proposed to be taken by Lucra to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects.

Such communication shall not be required if any of the following conditions are met:

(e) appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the Personal Data Breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);

(f) measures have been taken following the Personal Data Breach which ensure that the high risk to the rights and freedoms of the Data Subject is no longer likely to materialise; or

(g) it would involve disproportionate effort to contact Data Subjects. In which case a public communication or similar equally effective measure of communication to the Data Subjects shall be issued.

For any Personal Data Breach, a relevant supervisory authority may mandate that communication is issued to Data Subjects, in which case such communication must be issued.

20.5 **Press.** Lucra Personnel shall not communicate with the press and shall treat all potential Personal Data Breaches as confidential unless otherwise instructed in writing by the DPO. All press enquiries shall be directed to info@lucra.cc.

(a) If communication to the press is required, the following process shall be followed:

(i) the need for press communication is identified and wording drafted by the CEO (or, if not available, the non-executive chairperson);

(ii) appropriate channels of communication are identified (including accompanying social media statements where appropriate);

(iii) the draft press release is supplied to a relevant senior manager (board member);

(iv) the board member approves the press communication and channels of communication;

(v) all public facing staff are briefed on how to handle queries resulting from the press release; and

(vi) the communication is issued by the CEO (or, if not available, the non-executive chairperson).

21 Use of personal devices, applications or accounts for work purposes

Lucra Personnel are not permitted to use personal applications or accounts for work purposes. This includes, but is not limited to, personal email accounts and using third party applications which have not been approved for work use.

22 Changes to this Policy

We reserve the right to change this Policy at any time.