Man and Machine - Data Protection Policy

1. Introduction

This Policy sets out the obligations of Man and Machine Ltd, whose registered office is at Unit 8 Thame 40, Jane Morbey Road, Thame, Oxfordshire, OX9 3RR ("the Company") regarding data protection and the rights of individuals who are existing or potential customers, suppliers and other business contacts – including employees thereof ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 11).

3.2 The right of access (Part 12);

3.3 The right to rectification (Part 13);

3.4 The right to erasure (also known as the 'right to be forgotten') (Part 14);

3.5 The right to restrict processing (Part 15);

3.6 The right to object (Part 16); and

4. Lawful, Fair, and Transparent Data Processing

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, and states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in Part 17 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 17 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed of the purpose or purposes for which the Company uses their personal data. Please refer to Part 11 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

6.1 The Company will only collect and process personal data for (and to the extent necessary for) the specific purpose or purposes of which data subjects have been informed, or will be informed, as set out in Part 17, below.

6.2 Data we hold may be passed to respective software vendors for the necessary recording of Licence Information. We have ascertained the GDPR compliance of all vendors in our supply chain (see Section 22), and specifics can be obtained from their respective websites.

6.3 Any end-user data we receive from our resellers will only be used for the

purposes of processing orders via the aforementioned GDPR compliant third-party vendors.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 13, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Secure Processing and Data Retention

8.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 19 to 22 of this Policy.

8.2 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. (See Part 18 for details on our Data Retention policy)

8.3 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay. (See Part 20)

9. Accountability and Record-Keeping

9.1 The Company's Data Protection Officer is Paul Merchant, Finance Director

9.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

9.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

9.3.1 The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;

9.3.2 The purposes for which the Company collects, holds, and processes personal data;

9.3.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

9.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

9.3.5 Details of how long personal data will be retained by the Company; and

9.3.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. Data Protection Impact Assessments

10.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data

10.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

10.2.1 The type(s) of personal data that will be collected, held, and processed;

10.2.2 The purpose(s) for which personal data is to be used;

10.2.3 The Company's objectives;

10.2.4 How personal data is to be used;

10.2.5 The parties (internal and/or external) who are to be consulted;

10.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

10.2.7 Risks posed to data subjects;

10.2.8 Risks posed both within and to the Company; and

10.2.9 Proposed measures to minimise and handle identified risks.

11. Right of Data Subjects to be kept Informed

11.1 The Company shall provide the information set out in Part 11.2 to every data subject:

11.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

11.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

11.2 The following information shall be provided:

11.2.1 Details of the Company including, but not limited to, the identity of its Data Protection Officer;

11.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 17 of this Policy) and the legal basis justifying that collection and processing;

11.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

11.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

11.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

11.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;

11.2.7 Details of data retention;

11.2.8 Details of the data subject's rights under the GDPR;

11.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

11.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR); and

11.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

12. Right of Access

12.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

12.2 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

12.3 All SARs received shall be handled by the Company's Data Protection Officer.

12.4 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

13. Right for Rectification of Personal Data

13.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

13.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

13.3 If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

14. Right for Erasure of Personal Data

14.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

14.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

14.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

14.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 16 of this Policy for further details concerning the right to object);

14.1.4 The personal data has been processed unlawfully;

14.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation**.**

14.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 If any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

15. Right to Restriction of Personal Data Processing

15.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

15.2 If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

16. Right to Object to Personal Data Processing

16.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, and/or direct marketing.

16.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

16.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

17. **Personal Data Collected, Held, and Processed**

The following personal data is collected, held, and processed by the Company

Data Ref.	Type of Data	Purpose of Data
Contact Information	Names, addresses, phone numbers, job titles	To maintain contact with customers in the manner that would be expected in the normal course of business – to include ongoing support cases, news of product releases and updates, together with general day to day sales, finance and other similar contact.
Purchase History	Records of software and services purchased	To enable us to provide effective software licence contract management, appropriate support, consistency of service delivery
Support Cases	Details of support cases raised by Customers	To permit resolution of ongoing support issues, and history in case of repeat or related issues in future.
CRM Data	Meeting and phone conversation records	To enable us to interact efficiently with existing and potential customers in an ongoing manner, and to verify details of historical conversations with the Company
Marketing and Data Requests	Email addresses, and similar data captured via our website forms	To enable contact with parties who have opted into receiving marketing information from us.

18. **Data Retention Policy**

18.1 The Company shall not retain any personal data for any longer than is necessary considering the purpose(s) for which that data is collected, held, and processed.

18.2 Different types of personal data, used for different purposes, may be retained for different periods **(**and its retention periodically reviewed), as set out below.

18.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

18.3.1 The objectives and requirements of the Company;

18.3.2 The type of personal data in question;

18.3.3 The purpose(s) for which the data in question is collected, held, and processed;

18.3.4 The Company's legal basis for collecting, holding, and processing that data;

18.3.5 The category or categories of data subject to whom the data relates;

18.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

18.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

Data Ref. (see S17)	Retention Period or Criteria	Comments
Contact Information	6 years from most recent contact (invoice, conversation, or other communication)	Tax authorities require that relevant records are kept for at least 6 years. The rapid speed of change in our industry historically shows that customers and prospects may benefit from advancements in technology. Those businesses will only know that and become aware of those possibilities if they are kept informed of such advancements. We therefore consider that keeping existing and potential customers informed through our standard communications tools (email, newsletters, website, social media) is good business practice. In the absence of any known statistics, , we have assumed that 6 years is also a reasonable time period for individuals to remain in an organisation, and have used that as our benchmark retention period.
Purchase History		
Support Cases		
CRM Data		
Marketing and Data Requests	Deleted as soon as practically possible following notification from individual	

19. **Data Security – Communications and Storage**

The Company shall ensure that the utmost care is taken with respect to all communications and other transfers involving personal data. Furthermore, the Company shall ensure that the following measures are taken with respect to the storage of personal data:

19.1 All electronic copies of personal data should be stored securely on our internal servers and are only accessible by employees who are authorised to do so, via individual password access;

19.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media are stored securely on our premises;

19.3 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

20. **Data Security - Disposal**

Upon the expiry of the data retention periods set out below in Part 18 of this Policy, or

when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

20.1 Personal data stored electronically (including all backups thereof) shall be deleted;

20.2 Personal data stored in hardcopy form shall be shredded.

21. **Data Security - Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

21.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from a member of the Management Team;

21.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of a member of the Management Team;

21.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

21.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

21.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Management Team to ensure that the appropriate consent is obtained and that no data subjects have opted out.

22. **Organisational Measures**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

22.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

22.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

22.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data

22.3.1 will be appropriately trained to do so;

22.3.2 will be appropriately supervised;

22.3.3 shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

22.3.4 will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

22.3.5 must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

22.3.6 will have their performance regularly evaluated and reviewed;

22.4 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

22.5 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

22.6 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

23. Data Breach Notification

23.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

23.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

23.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 23.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

23.4 Data breach notifications shall include the following information:

23.4.1 The categories and approximate number of data subjects concerned;

23.4.2 The categories and approximate number of personal data records concerned;

23.4.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

23.4.4 The likely consequences of the breach;

23.4.5 Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

24. Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.