PAYWISER LIMITED

DATA PROTECTION POLICY

CONTENTS

1. Introduction

Paywiser Limited is a company incorporated in England and Wales under the company number 10677553 (the "Company"). The Company is committed to data protection and privacy. We respect and protects the rights of individuals, particularly the right to data protection and privacy as far as the processing and use of personal data is concerned. This Data Protection Policy ("Policy") is approved by the Board of Directors of the Company. The Data Protection Officer of the Company shall be responsible for the compliance and enforcement of data protection and privacy.

This Policy defines the standard for the data protection compliant processing of personal data. It defines the requirements for business processes that involve personal data and assigns clear responsibilities.

The Company must ensure that all processes involving the processing of personal data are able to fulfill the requirements stated in this Policy. As employers, the Company have the responsibility for the processing of their employees' personal data. When handling personal data in course of their duties, all employees of the Company are required to follow the requirements of this Policy.

The principles mentioned in this Policy are based on the European data protection and privacy laws and take into account the requirements of the EU **General Data Protection Regulation** (Regulation (EU) 2016/679 - GDPR). These principles apply to all staff members of the Company.

2. Definitions

- Anonymous data & Anonymized data
  Anonymous and anonymized data is data that does not refer to an identifiable natural person. Even if other data or additional information were added, identification of the natural person is not (or is no longer) possible. This Policy does not apply to such data.

- Biometric data

Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person (such as fingerprints or facial images).

- Consent
  Any freely given and unambiguous statement or other clear affirmative action by which the data subject indicates in an informed manner that he or she agrees to the processing of his or her personal data for a specific purpose.

- Controller
  Any natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data. For the personal data of its employees, customers, suppliers, partners, or other persons, Paywiser Limited is regarded as the controller.

- Data concerning health
  Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

- Erasure
  The irretrievable obliteration or physical destruction of saved personal data or its anonymization in such a way that makes it impossible to re-identify the natural person after the fact.

- Genetic data
  Personal data relating to the inherited or acquired genetic characteristics of a natural person that gives unique information about the physiology or the health of that natural person and which result in particular from an analysis of a biological sample from the natural person in question.

- Personal Data
  Any information relating to an identified or identifiable natural person ("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. Natural persons can be identified directly based on, for example, names, phone numbers, e-mail

addresses, postal addresses, user IDs, tax and social insurance numbers or indirectly through a combination of any other information. The personal data that is subject to this Policy includes data of employees, applicants, customers, suppliers and users of websites and services of the Company. It can be contained in the Company's own systems, in systems which third parties operate on behalf of the Company, or in the systems operated by the customers themselves, by the Company, or by third parties, to the extent that employees of the Company can gain access to the saved personal data there in the course of support and consulting activities.

- Processor
  A natural or legal person that processes personal data on behalf of the controller, such as an external service provider or a different Paywiser company that is not the controller itself.

- Processing
  Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The anonymization of data also represents a processing of personal data.

- Pseudonymization
  Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. Pseudonymized data constitutes personal data as defined in the GDPR; therefore, this Policy also applies to pseudonymized data.

- Special categories of personal data
  Certain personal data that is particularly sensitive due to its nature, whose processing is likely to result in significant risks for the rights of the data subject and therefore requires special protection. This includes data concerning health, Genetic data, biometric data processed to uniquely identifying a personal data, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, or sexual orientation. Depending on the context, this may also include data that could be misused for identity theft purposes, such as social security-, credit card-

and bank account numbers, ID-card or driver's license-numbers, also personal data regarding criminal investigation proceedings, convictions, and crimes, or data that is subject to professional confidentiality obligation.

- Third party
  A natural or legal person, public authority, agency, or body other than
  (a) the data subject,
  (b) the controller,
  (c) the processor and
  (d) the persons who are authorized to process personal data under the direct authority of the controller or processor.

- Recipient
  A natural or legal person, public authority, agency or another body, to which the personal data is disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with the laws of a particular jurisdiction shall not be regarded as recipients.

3. Principles for Protecting Personal Data

Personal data shall only be processed lawfully and in accordance with the principles set out below.

a. Lawfulness, Fairness, and Transparency
   Personal data may only be processed lawfully, fairly and in a transparent manner in relation to the data subject. This is the case when: processing is legally permitted in the specific case. Among others, the laws permit all cases of data processing that:

   - are necessary for the performance of contracts with the data subject (e.g. the storage and use of necessary personal data in the context of an employment- or service contract),

   - are necessary to take steps at the request of the data subject prior to entering a contract (e.g. a customer requests information about product X and then purchases said product. The data necessary to send the information material and to execute the contractual relationship may be processed),

- are necessary for compliance with legal obligations, e.g. due to tax or social insurance laws,

- are necessary to protect the vital interests of the data subject or of another natural person,

- are necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (e.g. for direct marketing),

- include decision-making based on automated processing in an individual case that produces legal effects concerning the data subject, when this automated decision is legally permitted, required for the performance of a contract with the data subject, or for which the data subject has explicitly granted consent, or

- when a data subject has granted his or her consent (for example, when registering on a website or subscribing to a newsletter).

Personal data should be collected directly from the data subject. If this is not the case, the data subject must be notified, particularly about the types of personal data that are being collected, processed, and/or used and for which specific purposes this occurs.

b. Specific Purpose

Personal data may only be collected for specific, explicit purposes. It may not be processed in a manner that is incompatible with those purposes.

The specific purpose must be defined before data collection. Processing for a purpose other than that for which the data have been collected is only permitted in exceptional cases, when a law permits processing for another purpose or if it is based on the data subject's consent. To ascertain whether the other purposes are compatible with the agreed purposes, the reasonable expectations of the data subject towards the Company with regard to such further processing, the type of data used, the possible consequences of the intended further processing for the data subject, and measures of encryption or pseudonymization must be taken into account.

c. Data Minimization

Personal data may only be collected to the extent which is absolutely necessary to fulfill the defined purpose. Processing must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed.

d. Accuracy

Personal data must be accurate and 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. All processes that involve the processing of personal data must provide an option for rectification and update.

e. Storage Limitation (Obligation to Erase)

Personal data may only be stored as long as is necessary for the purposes for which it is processed or due to other legal requirements, particularly to comply with statutory retention periods. After this point, personal data must generally be erased or anonymized. All processes for processing personal data must contain an option for erasure or blocking to the extent required by law.

f. Integrity, Availability, and Confidentiality

Personal data and its processing operations must always be appropriately protected by means of technical and organizational measures. This includes, in particular, suitable measures to protect against unauthorized or unlawful processing, accidental loss, destruction or damage, accidental disclosure and unauthorized access.

g. Processing of Special Categories of Personal Data

The collection, processing, and use of special categories of personal data should always be transparent for the data subject. Unless the collection and processing of such data is explicitly authorized by law, e.g. if necessary, for carrying out obligations and exercising rights in the field of employment, social security, social protection, it should only be collected on the basis of explicit prior notification and consent of the data subjects.

The consent must explicitly refer to these special data categories and their processing for one or more specified purposes. Unless applicable laws stipulate otherwise, special categories of personal data may only be processed and used with the explicit consent of the data subjects. Increased protective measures must be established to protect the data (e.g. physical security measures, access restrictions and encryption).

4. Rights of Data Subjects

a. Right to be informed

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. The Company must provide the data subjects with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with.

b. Right of Access and Data Portability

Data subjects have the right to obtain from the Company confirmation as to whether or not personal data concerning her or him are being processed. In such case, the Company shall provide for access as required by law. The information is provided in writing, unless the data subject submitted the request for information electronically. The information to be provided to the Data Subjects must include the purpose of storage, the recipients of the data, and all other legally required information pursuant to Article 15 of the GDPR. The data subject must be provided with a copy of the personal data that are undergoing processing. Upon request by the data subject, the data that he or she has provided to the controller must be made available in a structured, commonly used and machine-readable format.

c. Right to Rectification, Restriction, and Erasure

When personal data prove to be incorrect, incomplete, or out-of-date, each data subject has the right to rectification of his or her personal data. This can be the case, for example, if the data subject has changed history her name due to marriage.

Data subjects also have the right to obtain restriction of processing of their personal data when one of the following applies:

- The data subject contests the accuracy of the personal data and verification of the accuracy of the personal data takes some time. In this case, the data subject can demand restriction for the period of the verification of the accuracy.
- The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of its use instead.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims. Should it become apparent that certain information have a respective value to the

data subject, the data subject must be notified of the pending erasure with reasonable notice.

- The data subject has objected to processing for the duration of the clarification as to whether the legitimate interests for processing outweigh those of the data subject.

Within the restriction process, the stored personal data of the data subject must be marked with the aim to restrict access and limit their further processing. In addition, data subjects have the right to the erasure of their personal data in the following cases:

- The purpose of the data processing no longer applies.
- The data subject withdraws his or her consent for a specific purpose of processing.
- Address data is used for direct marketing purposes and the data subject objects to such use.
- The data is processed unlawfully.
- Erasure is required to meet legal obligations.

All processes in which personal data is collected, processed, or used must include a concept for the regular retention and deletion of personal data. This concept must ensure that personal data is erased in a timely manner after the fulfillment of the specified purpose or the lapse of the authorization for storage, particularly statutory retention terms. Instead of erasure, personal data may also be anonymized. If there is an obligation to erase personal data and said data has already been made public, other controllers shall be notified of the request to erase his or her data, including all links to this data.

d. Right to Object

Data subjects have the right to object to data processing when the Company processes personal data based on a decision in favor of its legitimate interests. In this case, the data subject must claim his or her own rights or interests on grounds relating to his or her particular situation, which outweigh the Company's legitimate interest to process the data. Data subjects can object to the processing of their personal data for purpose of direct marketing, including profiling if such is related to direct marketing, at any time and without giving reasons. If an objection is raised, the Company will not process this data further for these purposes. This does not apply where the processing cannot be ceased due to compelling legitimate grounds for the processing, particularly the establishment, exercise, or defense of legal claims.

e. Right to Complain

If a data subject wishes to file a complaint with regard to processing of her or his personal data, they can do so directly in an e-mail to the data protection officer: privacy@paywiser.com.

The data subject must be notified about all measures taken based on her or request within one month at the latest.

5. Data Protection Governance Structure

Responsibility for compliance with data protection requirements rests with the board of directors of the Company that processes the personal data for its business purposes. Executive management may delegate the task to fulfill this responsibility to managers at different levels within the organizational framework and the associated business processes.

6. Responsibilities for Data Protection Compliance

a. Management of Paywiser

The board of directors of the Company must ensure that the processes in their areas of responsibility in which personal data is processed (herein: “processes") meet the requirements of this Policy.

b. Employees

All employees are required to handle all personal data that they can access in the course of performing their duties for Paywiser Limited with strict confidentiality and to not collect, process, or use such data without authorization. Employees of the Company may only process personal data within the scope necessary to fulfill their duties as defined by their employment contracts. If the processing of personal data is not recognizably prohibited for an employee, he or she may assume the legality of the instructions from their superiors. When in doubt, employees should seek clarification from their managers.

.

7. Transfer/Commissioned Data Processing

If personal data is to be transferred to an associated company, a review must first take place as to whether contractual agreements regarding data protection and privacy are needed. Such review is required only when an associated company or external service

provider is to process personal data on behalf of the Company (referred to as “transfer for processing purposes"). If personal data that is to be transferred to a country outside the EEA, it must be ensured beforehand that an appropriate level of protection is guaranteed, pursuant to Article 44 of the GDPR.

In addition, the following rules apply to the transfer of personal data:

- **Transfer for commissioned processing:**
If the Company commissions an associated entity or an external company with the processing of personal data, it remains responsible for compliance with data protection and privacy requirements.

- **Transfer for the recipients’ own purposes:**
The Company may transfer personal data to an associated company or an external company for their own purposes only if this is legally permitted or required, or if the data subjects have first given consent.

8. Transfer of Customer Data

The Company processes personal data of customers and on behalf of customers. The use and, if relevant, transfer of such customer data must be in accordance with the applicable laws.