APPROPRIATE POLICY DOCUMENT

DATA PROTECTION POLICY

1. INTRODUCTION

This Data Protection Policy sets out how **Sanctuary of Sophia Ltd** ("we", "our", "us") process the personal data of our customers, prospects, suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

We commit to the correct and lawful treatment of personal data and to protecting the confidentiality and integrity of personal data.

All definitions used in this Data Protection Policy shall have the meaning given in the General Data Protection Regulation (*(EU) 2016/679*) (**"GDPR"**).

2. DATA PROTECTION PRINCIPLES

We adhere to the principles relating to the processing of Personal data set out in the GDPR which require personal data to be:

(a) processed lawfully, fairly and in a transparent manner (the Lawfulness, Fairness and Transparency principle);

(b) collected only for specified, explicit and legitimate purposes (the Purpose Limitation principle);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (the Data Minimisation principle);

(d) accurate and where necessary kept up to date (the Accuracy principle);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (the Storage Limitation principle);

(f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (the Security, Integrity and Confidentiality principle);

(g) not transferred to another country without appropriate safeguards being in place (the Transfer Limitation principle); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (the Accountability principle).

3. LAWFULNESS, FAIRNESS, TRANSPARENCY

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but

ensure that we process personal data fairly and without adversely affecting the Data Subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her consent;

(b) the processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

Where we process data under the legitimate interests ground at 4(e) above, the purposes for which we process personal data for legitimate interests are set out in our Privacy Notice.

We identify and document the legal ground being relied on for each processing activity and include this in our Privacy Notice.

3. CONSENT

A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal of such consent must be promptly honoured. Consent may need to be refreshed if we intend to process personal data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than explicit consent or consent if possible. Where explicit consent is relied on, we will issue a Privacy Notice to the Data Subject that requires signature of the Data Subject to obtain explicit consent.

We will evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

4. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The GDPR requires us as a Data Controller to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through our Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand it. You can view our Privacy Notice here Privacy Policy.
Whenever we collect personal data directly from Data Subjects, we must provide the Data Subject with all the information required by the GDPR including the identity of us as the Controller and of the DPO, how and why we will use, process, disclose, protect and retain that personal data. We do this through a Privacy Notice which must be presented when the Data Subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting or receiving the data. We must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

If we collect personal data from Data Subjects, directly or indirectly, then we will provide Data Subjects with a Privacy Notice.

5. PURPOSE LIMITATION

We will only collect and process personal data for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

We cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

6. DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

When personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines. You can see these Data Retention guidelines by clicking here.

7. ACCURACY

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

8. STORAGE LIMITATION

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

We will not keep personal data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

We will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all our applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in our Privacy Notice.

9. SECURITY INTEGRITY AND CONFIDENTIALITY

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable).

We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. We will implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. We will exercise particular care in protecting Special Categories of personal data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

We will follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. We may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it;

(b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed; and

(c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

10. REPORTING A PERSONAL DATA BREACH

The GDPR requires us as a Data Controller to notify any personal data breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected personal data breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

11. TRANSFER LIMITATION

The Data Protection Act 2018 restricts data transfers to countries outside the UK and the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal data is transferred originating in one country across borders when it is transmitted, sent, viewed or accessed in or to a different country.

We may only transfer Personal data outside the UK and the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;

(c) the Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their personal data. These include rights to:

(a) withdraw consent to processing at any time;

(b) receive certain information about the Data Controller's 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;

(i) object to decisions based solely on automated decision-making, 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.

We must verify the identity of an individual requesting data under any of the rights listed above and will not allow third parties to obtain personal data without proper authorisation.

13. ACCOUNTABILITY

We must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

We must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy and Privacy Notices;

(d) regularly training our employees on the GDPR, this Data Protection Policy, related policies and privacy guidelines and data protection matters including, for example, Data Subject's rights, consent, legal basis, DPIA and personal data breaches. We will maintain a record of training attendance by our employees; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

14. RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data processing activities.

These records will include, at a minimum, the name and contact details of us as the Controller and the DPO, clear descriptions of the personal data types, Data Subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. To create the records, we create a data map which includes the detail set out above together with appropriate data flows.

15. TRAINING AND AUDIT

We are required to ensure all of our employees have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

16. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

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 privacy principles.

We 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:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

We also conduct DPIAs in respect to high-risk processing.

We will conduct a DPIA when implementing major system or business change programs involving the processing of personal data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated decision-making including profiling;
- large-scale processing of Special Categories of personal data or Criminal Convictions Data; and
- large-scale, systematic monitoring of a publicly accessible area.

A DPIA includes:

- a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

17. AUTOMATED DECISION-MAKING

Generally, automated decision-making is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has explicitly consented;

(b) the processing is authorised by law; or

(c) the processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of personal data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but the Special Categories of personal data and Criminal Convictions Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on automated decision-making (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any automated decision-making (including profiling) activities are undertaken.

18. DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers or prospects.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

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

We comply with all of these rules on marketing.

19. SHARING PERSONAL DATA

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

We may only share the personal data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the personal data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

20. CHANGES TO THIS DATA PROTECTION POLICY

We keep this Data Protection Policy under regular review. This version was last updated on **09/01/2025**.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where we operate.

