Data Protection Policy (ISP-42)

1. Introduction

This Policy sets out the obligations of Serene Ltd. ("the Business"), registered in the UK regarding data protection and the rights of its customers, prospective customers, partners, and website users ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR") and the UKGDPR and corresponding articles within.

The UKGDPR defines "personal data" as any information relating to an identified or identifiable 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.

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

The Business 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

This Policy aims to ensure compliance with the UKGDPR.

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

a. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
b. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
d. 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.
e. 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.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UKGDPR in order to safeguard the rights and freedoms of the data subject.

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

a. The right to be informed
b. The right of access
c. The right to rectification
d. The right to erasure (also known as the 'right to be forgotten')
e. The right to restrict processing
f. The right to data portability
g. The right to object
h. Rights with respect to automated decision-making and profiling

4. Lawful, Fair, and Transparent Data Processing

The UKGDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject.

The UKGDPR states that processing of personal data shall be lawful if at least one of the following applies:

a. The data subject has given consent to the processing of their personal data for one or more specific purposes
b. 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
c. The processing is necessary for compliance with a legal obligation to which the data controller is subject
d. The processing is necessary to protect the vital interests of the data subject or of another natural person

e. 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
f. 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

The Business collects and processes the personal data, this Policy. This includes:

- Personal data collected directly from data subjects, and
- Personal data obtained from third parties

The Business only collects, processes, and holds personal data for the specific purposes as set out in the **General Privacy Notice** (or for other purposes expressly permitted by the GDPR).

Data subjects are kept informed at all times of the purpose or purposes for which the Business uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

The Business 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). Please refer to the relevant Data Privacy Notices for the determination of the types of data processing carried out by the Business.

7. Accuracy of Data and Keeping Data up to date

The Business 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 14, below.

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. Data Retention

The Business 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

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay

For full details of the Business's approach to data retention, including retention periods for specific personal data types held by the Business, please refer to our Data Retention Policy and relevant schedule contained therein. Additional data retention periods are defined within the accompanying Data Privacy Notices to this Data Protection Policy

9. Secure Processing

The Business 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 later in this Policy.

10. Accountability and Record-Keeping

The Business, by merit of processing PII, has appointed Privio as its Data Protection Officer.

The DPO's contact details are as follows:

- Email address: dpo@myserene.io
- Registered address: 62 Stakes Road, Purbrook, Waterlooville, Hampshire PO7 5NT).

These contact details can also be found in the various Data Privacy Notices accompanying this Data Protection Policy.

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

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

a. The name and details of the Business, its Data Protection Officer and any applicable third-party data processors
b. The purposes for which the Business collects, holds, and processes personal data
c. Details of the categories of personal data collected, held, and processed by the Business, and the categories of data subject to which that personal data relates
d. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards
e. Details of how long personal data will be retained by the Business (please refer to the Business's Data Retention Policy); and
f. Detailed descriptions of all technical and organisational measures taken by the Business to ensure the security of personal data

11. Data Protection Impact Assessments

The Business shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data where the specific requirements are met.

Data Protection Impact Assessments shall address the following:

a. The type(s) of personal data that will be collected, held, and processed
b. The purpose(s) for which personal data is to be used
c. The Business's objectives
d. How personal data is to be used
e. The parties (internal and/or external) who are to be consulted
f. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
g. Risks posed to data subjects
h. Risks posed both within and to the Business; and
i. Proposed measures to minimise and handle identified risks

12. Keeping Data Subjects Informed

The Business shall provide the information set out below to every data subject:

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
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

The following information shall be provided:

a. Details of the Business including, but not limited to, the identity of its Data Protection Officer
b. The purpose(s) for which the personal data is being collected and will be processed (as detailed in the **General Privacy Notice**) and the legal basis justifying that collection and processing
c. Where applicable, the legitimate interests upon which the Business is justifying its collection and processing of the personal data
d. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed
e. Where the personal data is to be transferred to one or more third parties, details of those parties
f. Details of data retention
g. Details of the data subject's rights under the GDPR
h. Details of the data subject's right to withdraw their consent to the Business's processing of their personal data at any time
i. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR)
j. 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; and
k. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences

13. Data Subject Access

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

Data subjects wishing to make a SAR may do so in writing, using the Business's Subject Access Request Form, or other written communication.

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.

All SARs received shall be handled by the Business's Senior Leadership Team.

The Business does not charge a fee for the handling of normal SARs. The Business 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.

14. Rectification of Personal Data

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

The Business shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Business 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.

In the event that 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.

15. Erasure of Personal Data

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

a. It is no longer necessary for the Business to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.
b. The data subject wishes to withdraw their consent to the Business holding and processing their personal data.
c. The data subject objects to the Business holding and processing their personal data (and there is no overriding legitimate interest to allow the Business to continue doing so) (see Part 18 of this Policy for further details concerning the right to object).
d. The personal data has been processed unlawfully.
e. The personal data needs to be erased in order for the Business to comply with a particular legal obligation.

Unless the Business 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.

In the event that 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).

16. Restriction of Personal Data Processing

Data subjects may request that the Business ceases processing the personal data it holds about them. If a data subject makes such a request, the Business 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.

In the event that 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).

17. Data Portability

The Business processes personal data using automated means. The Business uses a custom engine with a web interface, to manage and process customer data.

Where data subjects have given their consent to the Business to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Business and the data subject, data subjects have the right, under the UKGDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, the Business shall make available all applicable personal data to data subjects in the following format:

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. Objections to Personal Data Processing

Data subjects have the right to object to the Business processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the Business processing their personal data based on its legitimate interests, the Business shall cease such processing immediately, unless it can be demonstrated that the Business'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.

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

*Where a data subject objects to the Business processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, “demonstrate grounds relating to his or her particular situation”. The Business is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

The Business does not use personal data in automated decision-making processes unless deemed for a specific purpose as established in one or more of our corresponding Data Privacy Notices found on our web page or provided by us

20. Profiling

The Business does not use personal data for profiling purposes unless deemed for a specific purpose as established in one or more of our corresponding Data Privacy Notices found on our web page or provided by us.

21. Data Security – Transferring Personal Data and Communications

The Business shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data.

Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using postal delivery service; and

All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

22. Data Security – Storage

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

a. All electronic copies of personal data should be stored securely using passwords

b. All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar
c. All personal data stored electronically should be backed up daily with backups stored offsite; and
d. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Business or otherwise without the formal written approval of the DPO and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

23. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Business's Data Retention Policy.

24. Data Security – Use of Personal Data

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

a. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Business requires access to any personal data that they do not already have access to, such access should be formally requested from the **Data Protection Officer** or the **Information Security Office.**
b. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Business or not, without the authorisation of the **Data Protection Officer** or the **Information Security Office**
c. 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
d. 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
e. Where personal data held by the Business is used for technical support and providing an upgrade, it shall be the responsibility of the **Data Protection Officer** or the **Information Security Office** to ensure that the appropriate consent is obtained and that no data subjects have opted out.

25. Data Security – IT Security

The Business shall ensure that the following measures are taken with respect to IT and information security:

a. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
b. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Business, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.
c. All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Business's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible; and
d. No software may be installed on any Business-owned computer or device without the security check.

26. Organisational Measures

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

a. All employees, agents, contractors, or other parties working on behalf of the Business shall be made fully aware of both their individual responsibilities and the Business's responsibilities under the UKGDPR and under this Policy, and shall be provided with a copy of this Policy
b. Only employees, agents, sub-contractors, or other parties working on behalf of the Business 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 Business.
c. All employees, agents, contractors, or other parties working on behalf of the Business handling personal data will be appropriately trained to do so.
d. All employees, agents, contractors, or other parties working on behalf of the Business handling personal data will be appropriately supervised.
e. All employees, agents, contractors, or other parties working on behalf of the Business handling personal data 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.
f. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
g. All personal data held by the Business shall be reviewed periodically, as set out in the Business's *Data Retention Policy*.

h. The performance of those employees, agents, contractors, or other parties working on behalf of the Business handling personal data shall be regularly evaluated and reviewed.
i. All employees, agents, contractors, or other parties working on behalf of the Business handling personal data will be bound to do so in accordance with the principles of the UKGDPR and this Policy by contract.
j. All agents, contractors, or other parties working on behalf of the Business handling personal data 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 Business arising out of this Policy and the GDPR; and
k. Where any agent, contractor or other party working on behalf of the Business handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Business against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27. Transferring Personal Data to a Country Outside the EEA

The Business is based in the UK and therefore any personal data provided to the Business will be stored and processed within the UK.

Should we use providers based in a third Country, we may transfer data to them if they are part of any equivalence measures or with the inclusion of Standard Contract Terms under UKGDPR which requires them to provide similar protection to personal data shared between Europe and the applicable Third Countries.

If none of the above safeguards is available, we may request your explicit consent to the specific transfer. You will have the right to withdraw this consent at any time.

Please email us at the contact address given if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

28. Data Breach Notification

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

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 DPO 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.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

a. The categories and approximate number of data subjects concerned
b. The categories and approximate number of personal data records concerned
c. The name and contact details of the Business's DPO (or other contact point where more information can be obtained)
d. The likely consequences of the breach
e. Details of the measures taken, or proposed to be taken, by the Business to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Version Control

Title	Data Protection Policy ISP-42			
Description	Policy Document			
Created By	Information Security Office			
Date Created	2025			
Maintained By	Information Security Office			
Approved By	Board of Directors			
Version Number	**Modified By**	**Modifications Made**	**Date Modified**	**Status**
1.0	ISO	Initial creation	2024	Superseded
2.0	ISO	Reviewed for 2025 Audit purposes - format overhauled	04/2025	Superseded
2.0	ISO	Annual review - no changes required	04/2026	Live