Privacy Policy

Policy Name	Privacy policy
Policy Owner	Chief Risk Officer
Contact Person	Compliance Officer
Applicability	All areas
Stakeholders / Interested Parties	
Original Issue Date	
Current Version Issue Date	
Version No.	V8
Approval Committee	Directors Aicura Solutions
Date Approved	July 2025
Next Review Date	

Table of Contents

1. Purpose of our Policy

Aicura Solutions, (Company number 07998395) (**Aicura, we**, **us**, or **our**) provides the products and services offered on the Aicura website and Vaultigo platform**.** to our customers (individual, you).

For the purposes of the Data Protection Act 2018 (Act) and General Data Protection Regulation (GDPR), accountability rests with our Data Protection Officer (DPO) by assisting with the sharing of information between customers and associated GDPR compliant services, as well as managing the customer's ultimate experience.

We have adopted this policy to ensure that we have standards in place to govern how we gather, manage, protect, use and store the data about individuals that is necessary and incidental to:

- providing the products and services that we offer; and
- the normal day-to-day operations of our business.

By publishing this policy, we aim to be transparent in our dealing with customer data and information, make it easy for our users, customers and the public to understand what data we collect and store, why we do so, how we receive and/or obtain that information, and the rights customers have with respect to consenting and managing their data in our possession.

2. Who and What This Policy Applies To

- We handle data in our own right and also for and on behalf of our customers and users.
- This policy applies to all persons, both natural and legal, where we request input of information and store it for use of our platform and associated services in order to maximise and enhance the customer experience of use of the platform.
- The policy applies to all forms of information, physical and digital, whether collected or stored electronically or in hardcopy.
- If, at any time, an individual provides data or other information about someone other than himself or herself, the individual warrants that they have that person's consent to provide such information for the purpose specified.
- Any individual/s who access the Aicura website and Vaultigo platform are required to expressly consent to use of their data, but which may also be removed and forgotten through stipulation by the individual.
- Aicura is not available to children (persons under the age of 18 years), or where a child is involved, express guardian consent is required.

3. The Information We Collect

In the course of business, it is necessary for us to collect data in order to maximise and enhance our customer's experience. The information we collect allows us to identify who an individual is for the purposes of our business, share data when legally asked of us, contact the individual in the ordinary course of business and transact with the individual. The types of information we may collect is:

- **Personal Information.** We may collect personal details such as an individual's name, location, date of birth, photograph, passport, driver's license and other information that allows us to identify who the individual is;
- **Contact Information.** We may collect information such as an individual's email address, mobile and/or landline telephone number, third-party usernames, residential and business address, and other information that allows us to contact the individual and the individuals they name as valid contacts as a part of Aicura usage.
- **Financial Information.** We may collect financial information related to an individual about payments made and received (including invoicing), such as the date, amount, currency and the details of the payee or payer and other information that allows us to transact with the individual and/or provide them with our services;
- **Statistical Information.** We may collect information about an individual's online and offline preferences, habits, movements, trends, decisions, associations, memberships, finances, purchases and other information for statistical purposes;

- **Device Information.** We collect device-specific information, such as the hardware model, operating system version, advertising identifier, unique application identifiers, unique device identifiers, IP addresses, browser type, language, wireless network, and mobile network information (including the mobile phone number); and
- **Information an individual sends us.** We may collect any personal correspondence that an individual sends us, or that is sent to us by others (such as credit reference or fraud prevention agencies) about the individual's activities, including activities with our third-party partners.

We may collect other data about an individual, which we will maintain in accordance with this policy. Where data is collected, express consent to do so is to be obtained from the customer, not withstanding an express notice of withdrawal of any / all information stored at any point in time.

We may also collect anonymous non-data about an individual such as information regarding their computer, network and browser.

We do not collect any special categories of personal data, such as race, religion, political opinion, trade or other union membership, sexual orientation, health information, biometric or genetic data as none of these are relevant to the types of work we carry out as part of our day-to-day business operations.

4. How Information Is Collected

All of the information we collect is in association with an individual's use of Aicura, our platform, products and services, an enquiry about Aicura or by generally dealing with us, and is collected as follows:

- **Registrations/Subscriptions/Purchases.** When an individual registers, subscribes, and or purchases a product, service, list, account, connection or other process whereby they enter data details or grant access to information in order to receive or access something, including a transaction or services;
- **Accounts/Memberships.** When an individual submits their details to open an account and/or become a member with us;
- **Partners.** When an individual grants us access to their accounts or allows information to be shared by our business partners.
- **Supply/Contact.** When an individual supplies us with goods or services**.** or contacts us in any way;
- **Pixel Tags.** Pixel tags and web beacons may enable us to send email messages in a format customers can read and they tell us whether mail has been opened.
- **Shareholder Information.** We collect information from each of our shareholders, such as the name, date of birth and address.

As there are many circumstances in which we may collect information both electronically and physically, we will endeavour to ensure that an individual is always aware of their data being collected, in particular by third parties, is able to consent to use of their data by third parties, manage their consents for each third party, and withdraw collection of their data at any point with third parties.

We may also collect anonymous non-data, which may be used and shared on an aggregated and anonymous basis – this non-data holds no customer detail or information about the customer.

5. How Data Is Stored

The data that we collect from you will be stored in the United Kingdom, in a secure, end-to-end encrypted data store maintained with the Google UK Data Centre.

Data may also be processed by third parties and/or staff operating outside the EEA who work for us or for one of our third-party partners. Such staff may be engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting and consenting to provide your personal data, you agree to this transfer, storing or processing.

We will retain data for the period necessary to fulfil the purposes outlined in this policy unless a longer retention period is required or permitted by law.

By consenting to our Privacy Policy, you agree to this transfer, storing or processing.

6. When Data Is Used

We will only use any data for the purpose for which it was collected, and for which the individual's permission was given. The purpose of collection is determined by the circumstances in which the information was collected and/or submitted.

Information is used to enable us to operate our business, especially as it relates to an individual. This may include:

- The provision of Aicura and related services to an individual;
- Verifying an individual's identity;
- Communicating with an individual about:
    - Their relationship with us;
    - Our services;
    - Our marketing and promotions to customers and prospects; and/or
- Competitions, surveys and questionnaires;
- Marketing and promotions to customers and prospects;
- Investigating any complaints about or made by an individual, or if we have reason to suspect that an individual is in breach of any of our terms and conditions or that an individual is or has been otherwise engaged in any unlawful activity;
- Carrying out regulatory checks and meeting our obligations to our regulators;
- Preventing and detecting fraud, money laundering and other crime (such as identity theft);
- Preparing high-level anonymised statistical reports, which would contain details such as the average number of company directors being authorised signatories to a company's accounts. The information in these reports is never personal and you will never be identifiable from them. We may share these statistical and anonymised reports with third parties including non-Aicura companies; and/or
- As required or permitted by any law (including the Act).If you publicly post about Aicura, or communicate directly with us, on a social media website, we may collect and process the data contained in such posts or in your public profile for the purpose of addressing any customers services requests you may have and to monitor and influence public opinion of Aicura, subject to the appropriate consent being in place.

7. When Data Is Disclosed

Data is only disclosed where required, such as:

- Upon your authorisation and instruction, to your advisers (such as accountants, lawyers, financial or other professional advisers).
- Where legally bound, or in accordance with the Act, it may be necessary for us to disclose an individual's data in the course of our business, such as for processing activities like verification, due diligence, website hosting, data analytics and payment processing. Where we employ other companies to perform tasks on our behalf and we need to share your information with them to provide products and services to you. You will be notified of these instances and requested to authorise access to these products or services.

There are some extreme circumstances in which we must disclose an individual's information, especially as it relates to:

- Where we reasonably believe that an individual may be engaged in fraudulent, deceptive or unlawful activity that a governmental authority should be made aware of;
- As required by any law (including the act) including court orders;
- As required by UK and overseas regulators and authorities in connection with their duties, including the regulator or authority having access payment details (including information about others involved in the payment);
- Fraud prevention agencies, in particular, we will always tell fraud prevention agencies if you give us false or fraudulent information. They will also allow other organisations (in the UK or abroad), including law enforcement agencies to access this information to prevent and detect fraud, money laundering or other crimes; and/or

- In order to sell our business (as we may transfer data to a new owner).

We will not disclose an individual's data to any entity outside of the United Kingdom that is in a jurisdiction that does not have a similar regime to the Act or an implemented and enforceable privacy policy similar to this policy. We will take reasonable steps to ensure that any disclosure to an entity outside of the United Kingdom will not be made until that entity has agreed in writing with us to safeguard data as we do.

If the Company gets involved in a merger, asset sale, financing, liquidation or bankruptcy, or acquisition of all or some portion of the business to another company, we may share information with that company before and after the transaction closes.

8. Roles and Responsibilities

- Aicura's responsibilities
    a. Aicura is the data processor under Data Protection Act for the personal data it processes on behalf of its client.
    b. the Accounting Officer has overall responsibilities for compliance with data Protection legislation;
    c. the Data Protection Officer (DPO) is responsible for training, monitoring progress and advising the organisation on implementation of this policy; acting as primary contact on any data protection queries;
    d. Aicura provides appropriate separation of duties to allow the DPO to supervise compliance with GDPR;
    e. the DPO will conduct regular assurance activity to monitor and assess new processing of personal data;
    f. the DPO will monitor and report on all data processor requirements e.g. Roles & Responsibilities, notification;
    g. the DPO is the first point of contact for the regulatory authorities and for individuals whose data is processed (employees, customers etc.).
- Employee responsibilities
    a. All employees have individual responsibility for complying with this policy and following accompanying guidance.
    b. All employees will undertake relevant data protection training and any other training that shall be deemed as mandatory.
    c. Employees will:
        - observe all forms of guidance, codes of practice and procedures about the collection, sharing, handling and use of personal information;
        - develop a comprehensive understanding of the purpose for which Aicura uses personal information;
        - collect and process information in accordance with the purpose for which it is required to be used by Aicura to meet its statutory requirements and business needs;
        - ensure the information is destroyed when no longer required in line with our information management guidance and client requests.
        - understand that breaches of this policy may result in scrutiny by the Information Commissioner's Office (ICO) with the potential for fines to be levied and accompanying reputational damage. There is also the potential for misconduct action.

9. Data Protection Impact Assessments

- A Data Protection Impact Assessment (DPIA) will be carried out if a project or the introduction of a new service or policy is likely to result in a high risk to the privacy of individuals. A DPIA is a process that helps identify privacy risks and ensure lawful practice when a new project is designed, or changes are made to an existing service or policy.
- The purpose of the DPIA is to ensure that privacy risks are mitigated including promptly addressing any identified issue while allowing the aims of the project or policy to be met whenever possible.
- According to the Information Commissioner's Office, a DPIA is required when an organisation plans to:
    - embark on a new project involving the use of personal data;
    - introduce new IT systems for storing and accessing personal information;
    - participate in a new data-sharing initiative with other organisations;
    - use profiling or special category data to decide on access to services;
    - initiate actions based on a policy of identifying particular demographics;
    - use existing data for a new and unexpected or more intrusive purpose;
    - match data or combine datasets from different sources;
    - collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
    - profile children or target services at them; or
    - process data that might endanger the individual's physical health or safety in the event of a security breach;
    - continue to utilise long standing databases where the DPIA may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues.
- Guidance issued by the Information Commissioner's Office on DPIAs can be found on the ICO website.

10. Data protection by Design and Default

- In compliance with data protection by design principle, we will ensure data protection risks are taken into account throughout the process of designing a new process, product, policy or services, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure the processing complies with the law and protects the rights of the data subjects.
- To comply with data protection by design and by default principles, we will ensure mechanisms are in place within the organisation to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.
- Read the guidance on data protection by design and default

11. Third Party Services, Websites and Accounts

We will not disclose, share or sell any collected customer information with any third parties, except where our services and offerings have been set up and configured by our customers, and where the set up enhances the overall customer experience.

We may link your account with a third party to our services to enable certain functionality, which allows us to obtain information from those accounts. You will be notified of these instances and requested to authorise access to these products or services.

For example, we may share an individual's information as follows:

- Authentication of identity, passport and driver's license (such as AU10TIX, Onfido, Oracle Watchlist);
- All information may be processed and stored with cloud service providers (such as Amazon Web Services);
- Information may be required to communicate with an individual (such as Gmail from Google, Inc);
- To assist marketing and promotions to other customers and prospects on social media (such as Facebook or Instagram);
- In relation to the provision of a cross-border payment solution
- In relation to fraud monitoring solutions employed by Aicura

When you click on links to third party websites, we may link your account with a third party to our services to enable certain functionality, which allows us to obtain information from those accounts.

While managing our own use of customer data, we will ensure alignment of our services with all partner third parties, however, we are not responsible for the privacy practices of third parties. It is your responsibility to read the privacy policies of third party service providers, so you can understand the manner in which they will handle your personal information. The information we may obtain from those services often depends on their privacy policies or account settings.

These service providers may be located or have facilities that are located a different jurisdiction (including outside the EEA), in which case your information may become subject to the laws of the jurisdiction(s) in which that service provider or its facilities are located.

12. Cookie Policy

Our Platform may use cookies to distinguish you from other users of our Platform. This helps us to provide you with a good experience when you browse our Platform and also allows us to improve our Platform. Your consent will be obtained prior to our use of cookies on our Platform and you are able to revoke that consent following the procedure below.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your device if you agree. Cookies contain information that is transferred to your device's hard drive. You block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our Platform for which we require the use of cookies.

13. Consent to Collection of Data

An individual may opt to not have us collect their data and communicate with them at certain times. This may prevent us from offering them some or all of our services and may terminate their access to Aicura, or other services they access with or through us.

- **Opt In.** Where relevant, the individual will have the right to choose to have information collected and/or receive information from us; or
- **Opt Out.** Where relevant, the individual will have the right to choose to exclude himself or herself from some or all collection of information and/or receiving information from us. An individual may revoke their consent at any time, and the decision to opt out will be made through the same media by which the individual opted in.
- **Opt to be forgotten.** Where relevant, the individual will have the right to choose to be completely forgotten / removed from a service so that no further access, communication or storage of data will be maintained.

If an individual believes that they have received information from us that they did not opt in or out to receive, or where they have requested to be forgotten, they should contact us on the details below.

14. The Safety & Security of Data

We will take all reasonable precautions to protect an individual's data from unauthorised access. This includes appropriately securing our physical facilities and electronic networks.

The security of online transactions and the security of communications sent by electronic means or by post cannot be guaranteed. Each individual that provides information to us via the internet or by post does so at their own risk. We cannot accept responsibility for misuse or loss of, or unauthorised access to, data where the security of information is not within our control.

We are not responsible for the privacy or security practices of any third party (including third parties that we are permitted to disclose an individual's data to in accordance with this policy or any applicable laws). The collection and use of an individual's information by such third parties may be subject to separate privacy and security policies, as maintained by that third party.

If an individual suspects any misuse or loss of, or unauthorised access to, their data, they should let us know immediately.

We are not liable for any loss, damage or claim arising out of another person's use of the data where we were authorised to provide that person with the data through the managed consent process.

15. How to Access and / or Update Information

The Act gives you the right to request from us the data that we have about you.

If an individual cannot update his or her own information, we will correct any errors in the data we hold about an individual within one month of receiving written notice from them about those errors.

It is an individual's responsibility to provide us with accurate and truthful data. We cannot be liable for any information that is provided to us that is incorrect.

We may charge an individual a reasonable fee for our costs incurred in meeting any of their requests to disclose the data we hold about them, if such a request is manifestly unfounded or excessive. We reserve the right to clarify the specific information your request relates to.

Information will be provided within one month of receipt of the request.

16. Complaints and Disputes

You have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing; and
- Processing for purposes of scientific/historical research and statistics
- Unless we hold compelling legitimate grounds for processing or the processing is for the establishment, exercise or defence of legal claims.

If an individual has a complaint about our handling of their data, they should address their complaint in writing to the details below.

You have the right to lodge a complaint with a supervisory authority if you consider that the processing of your data infringes the General Data Protection Regulation.

If we have a dispute regarding an individual's data, we both must first attempt to resolve the issue directly between us.

If we become aware of any unauthorised access to an individual's data which is likely to result in a high risk for the rights and freedoms of the data subjects, we will inform the individual without undue delay after becoming aware of it, once we have established what was accessed and how it was accessed.

17. Additions to this Policy

We reserve the right to modify this policy at any time, so please review it frequently. Changes and clarifications will take effect immediately upon their posting on the Platform. If we make material changes to this policy, we will notify you here that it has been updated, so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we use and/or disclose it.

If we decide to change this policy, we will post the changes on our Platform at www.aicurasolutions.com/privacy. It is your responsibility to refer back to this policy to review any amendments. We may do things in addition to what is stated in this policy to comply with the Act and nothing in this policy shall deem us to have not complied with the Act.

18. Contacting Us

All correspondence relating to privacy should be addressed to (by email where possible):

info@aicurasolutions.com

Data Protection Officer
Aicura Limited
52 Grosvenor Gardens
London
England
SW1W 0AU