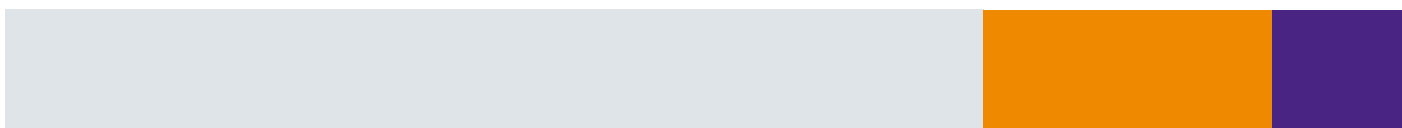


GDPR AND PRIVACY POLICY

April 2026

POLICY DETAILS		
POLICY CODE:	PVC-FDA-GDPR.1	
DEPARTMENT:	DATA PROTECTION	April 2026
POLICY OWNER:	ADRIAN DAWKES	<small>Signed by:</small> <i>Adrian Dawkes</i> <small>33128E6E95834B7</small>
APPROVED BY:	FINTAN WALTON	<small>DocuSigned by:</small> <i>Fintan Walton</i> <small>414B502686854A5</small>
EFFECTIVE DATE:		
REVIEW PERIOD:	One year from approval	



1. GDPR AND PRIVACY POLICY

While conducting its business PharmaVentures Ltd. ("PharmaVentures") collects stores and processes information regarding employees, business partners and other third parties. Where this relates to individuals, it is "personal data" under the Data Protection Act 1998 (the "DPA") and GDPR (General Data Protection Regulation 2018) and subsequently amended by the Data Use and Access Act 2025 (DUAA), the use of which is subject to legal restrictions. Under GDPR entities that process such data are considered as either Controllers or Processors, the definition of which is stated below

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"

The firm considers itself to be a controller for the purposes of the GDPR.

2. FAIR AND LAWFUL PROCESSING

GDPR is intended not to prevent the processing of personal data, but rather to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the firm) and who the data controller's representative is (in this case the Data Protection Officer or equivalent), the purpose for which the data is to be processed by the firm, and the identities of anyone to whom the data may be disclosed or transferred.

For Personal Data to be processed lawfully, certain specific conditions must be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.

- Processing may be necessary for the performance of a contract or to take steps to enter a contract.
- Processing may be necessary for compliance with a legal obligation
- 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 controller.
- Necessary for the legitimate business interests pursued by the controller or a third party except where such interests are overridden by the interests, rights or freedoms of the data subject.

3. PERSONAL DATA AND THE DATA PROTECTION PRINCIPLES

The firm, its employees and other persons working for it (including contractors, consultants and temporary staff) need to be aware of the requirements to be followed when handling Personal Data (and Sensitive Personal Data) so as to protect the rights of the individual to whom that personal information relates.

When processing Personal Data, the following eight data protection principles must be followed. Personal Data must:

1. be processed fairly and in accordance with applicable laws;
2. be processed for specified purposes and in an appropriate way;
3. be adequate, relevant and not excessive;
4. be accurate and kept up to date;
5. be kept for no longer than is necessary;
6. be processed in line with the rights of the individual;
7. be kept secure at all times; and
8. only be transferred to countries outside the European Economic Area only where the data protection regime of the country in question provides adequate protection for personal information, and permission from the individual concerned has been obtained.

4. PHARMAVENTURES APPLICATION

PharmaVentures is committed to protecting client privacy and takes its responsibility regarding the security of customer information very seriously. We will be clear and transparent about the information we are collecting and what we will do with that information.

This Privacy Policy does not affect the agreements between PharmaVentures and its affiliates and its various clients which are subject to separate written agreements which may supersede this general GDPR & Privacy Policy.

By using www.pharmaventures.com ('Site'), other software applications or any of our services or otherwise providing information to PharmaVentures, external parties are agreeing to our Privacy Policy. If at any time they do not agree with this policy, then they have the right to request the removal/deletion of any and all personal data we may hold. **This Policy sets out the following:**

- What personal data PharmaVentures collects and process about individuals in connection with a relationship with us as a client and/or through your use of our website or other services;
- Where we obtain the data from;

- What we do with that data;
- How we store the data;
- Who we transfer/disclose that data to;
- How we deal with your data protection rights;
- And how we comply with the data protection rules.

All personal data is collected and processed in accordance with EU data protection laws

PharmaVentures Limited acts as a data controller. “Pharma Ventures Ltd.” (referred to as “we”, “us”, “our”, or most commonly referred to as “PharmaVentures” in this policy) in this policy primarily refers to Pharma Ventures Ltd, registered in England and Wales under Company Number 03419584 and whose registered office is c/o Gravita Oxford LLP, First Floor, Park Central, 40-41 Park End Street, Oxford, OX1 1JD.

5. WHAT RIGHTS DO INDIVIDUALS HAVE OVER THEIR PERSONAL DATA?

1. Under the General Data Protection Regulation, any individual has the right to:
 - To be informed
 - Data portability
 - Matters in relation to automated decision making and profiling
 - Access their personal data by making a subject access request
 - Rectification, erasure or restriction of the information where this is justified
 - Object to the processing of the information where this is justified
 - Erasure of information (the right to be forgotten)
 - The right to erasure (the right to be forgotten)
2. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following applies:
 - a) The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - b) The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
 - c) The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
 - d) The personal data have been unlawfully processed;

- e) The personal data must be erased for compliance with a legal obligation in a Union or Member State law to which the controller is subject;
 - f) The personal data had been collected in relation to the offer of information society services referred to in Article 8(1).
3. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
4. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
- a) for exercising the right of freedom of expression and information;
 - b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
 - d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - e) For the establishment, exercise or defence of legal claims. **Exercising Rights**

For an individual to exercise their rights they should contact PharmaVentures using the following contact details:

PharmaVentures Limited
c/o Gravita Oxford LLP,
First Floor, Park Central,
40-41 Park End Street,
Oxford,
OX1 1JD

or

Email: privacy@pharmaventures.com

6. THE PERSONAL DATA PHARMAVENTURES COLLECTS:

Where we collect data that identifies an individual this is classed as “personal data”. Personal data may include (but is not limited to) a name, date of birth, contact address and telephone number.

The types of personal data we may request are:

- Full name and Title, Job Title, Department
- Contact information such as postal address, email address and telephone numbers
- Marketing preferences which include the type of information an individual may wish to receive and how.

- Information we learn from individuals such as requests, transactions, services provided or offered, any advice or recommendations made, a log of meetings, telephone recordings (where permitted and required for regulatory purposes) complaints and dissatisfaction notes, as well as email exchanges.

The above list is not exhaustive, and we may from time to time require additional information in order to satisfy our legal and regulatory obligations or fulfil the obligations of a specific contractual arrangement with a client for the provision of services by us. Where additional information is required, we will provide a reasonable explanation of why it is required unless we are prevented from doing so by law.

PharmaVentures may use methods such as pseudonymization, which is a process whereby we can replace identifying fields of data with other non-identifying data fields in order to anonymise the data from the individual therefore meaning the data is no longer personal. We may use this method where we are required to retain certain types of information for clients, such as number of females and males employed, jobs created, and average salaries paid. This type of statistical data is often required for ESG (Environmental, social and governance) investment purposes by clients to show value added investments made by the firm on behalf of its clients.

Use of PharmaVentures website:

The type of data we collect when an individual visits our website may include internet protocol addresses, browser type and version, browser plug-in types and versions, time zone setting and location, operating system and platform and other technology on the devices used to access this Site as well as the types of products and services and searches conducted on our Site.

Special Category Data:

Special Category data refers to any data which is sensitive and is subject to additional rules and requirements under the General Data Protection Regulations. Special category data may include information regarding: Criminal convictions and offences, race, ethnicity, religious or philosophical beliefs, political opinions, sexual orientation, trade union membership and information about an individual's health, genetic and biometric data.

As a general rule we do not collect any Special Category Data. However, we are required to request information relating to criminal convictions as part of our recruitment process for staff and contractors undertaking regulated activities and as such, we require consent from the individual for this. If we are required by law to request any special category data, aside from the reasons mentioned above we will provide a reasonable explanation as to the nature and purpose for this request and obtain appropriate consent.

How do we collect personal data?

Typically, where we are required to obtain an individual's personal data, we will request it from the individual or a business card, vCard or electronic method where provided. However, we may also from time to time receive personal data through intermediaries where the sharing of the data has been appropriately authorised. Intermediaries may include Accountants, Solicitors, Independent financial advisors, Tax advisors and wealth managers. Personal data may be provided to us via post, in person, email or via a specially created secure data room / platform. The data collection may be facilitated by

way of completing an application form or questionnaire or by responding to information requests from us. We may also receive information from publicly available resources. Cookies may be used when accessing the company website for statistical analysis.

Why do we collect personal data?

We only collect personal data where we believe we have a legitimate business interest in common with an individual or we have a lawful purpose to do so. These reasons may include but may not be limited to circumstances where an individual:

- Is a legitimate interested or potentially interested party to a licensing, M&A, fundraising or related opportunity;
- Is a shareholder in one of the companies to whom we have an administration and / or management agreement with or have a contractual agreement with;
- Is actively receiving investment services or products from us under a contractual arrangement or engagement.
- Has consented to receiving communications from us
- Has or has had a contractual agreement with us
- Requests resources or marketing be sent;
- Gives us feedback or some other form or legitimate business interest communication.

How and why do we use personal data:

Typically, we only use the data to be able to perform our duties under contracts we may have with individuals or businesses or where it is necessary for our legitimate interests (or those of a third party) and any individuals interests and fundamental rights do not override those interests.

Generally, we do not rely on consent as a legal ground for processing personal data, other than in relation to sending marketing communications via email or text message. Individuals have the right to withdraw consent to marketing at any time by emailing us at privacy@pharmaventures.com or using the appropriate "Opt Out" link on any communication.

We may process personal data for more than one lawful ground, depending on the specific purpose for which we are using the data.

Marketing communications:

Individuals may receive marketing communications from us if they have:

- I. requested information from us or have or have had a contractual agreement with us; or
- II. if an individual provided us with your details and have positively consented to us sending you marketing communications; and
- III. in each case, the individual has not opted out of receiving that marketing.

We will obtain express opt-in consent before we share any individual's personal data with any third party for marketing purposes. That consent is not infinitive, and individuals can opt-out from receiving marketing communication from us at any time by emailing; privacy@pharmaventures.com

Where an individual has opted out of receiving our marketing communications, this will not apply to communication we make with that individual in relation to a legitimate business interest or lawful purposes, such as the performance of an existing or future contract.

Change of purpose:

We will only use personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use personal data for a purpose unrelated to the purpose for which we collected the data, we will notify the individuals concerned and explain the legal grounds for this.

We may process personal data without an individual's knowledge or consent only where this is required and permitted by law.

7. SHARING AND DISCLOSURE OF PERSONAL DATA:

We may share personal data with the parties set out below for legitimate business interests and lawful purposes, these may include but are not limited to:

- Other companies in our group who provide IT and system administration services and undertake leadership reporting. Service providers who provide IT and system administration services.
- Professional advisers including lawyers, bankers, auditors, tax advisors and insurers who provide consultancy, banking, legal, insurance, tax and accounting services.
- HM Revenue & Customs, regulators and other authorities based in the United Kingdom and other relevant jurisdictions who require reporting of processing activities in certain circumstances which may include but is not limited to The Financial Conduct Authority.
- Fraud prevention agencies,
- Third parties to whom we sell, transfer, or merge parts of our business or our assets.

We require all third parties to whom we transfer your data to respect the security of personal data and to treat it in accordance with the law. We only allow such third parties to process personal data for specified purposes and in accordance with our instructions.

Where we transfer any data outside of the EEA it is only done so to fulfil a contractual obligation and in a way which maintains compliance with GDPR legislation.

8. DATA SECURITY:

We have put in place adequate, proportionate and appropriate security measures as is required of an authorised firm to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal data to those employees, agents, contractors and other third parties who have a business need to know such data. They will only process personal data on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with data breaches in accordance with the GDPR (General Data protection regulation) and we will notify individuals and any applicable regulator of a breach where we are legally required to do so.

Data Retention periods:

We will only retain personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we must keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years for tax purposes and for at least five years after a client ceases to be a client under the UK money laundering regulations 2017.

In some circumstances we may pseudonymise personal data for statistical purposes in which case we may use this information indefinitely without further notice.

9. GDPR PERSONAL RIGHTS:

Under certain circumstances, individuals have rights under data protection laws in relation to personal data. These include the right to:

- To be informed
- Data Portability
- Matters in relation to automated decision making and profiling
- Rectification, erasure or restriction of the information where this is justified
- Request access to personal data (Subject access request).
- Request correction of personal data.
- Request erasure of personal data.
- Object to processing of personal data.
- Request restriction of processing personal data.
- Request transfer of personal data.
- Right to withdraw consent.

For further information or to exercise any of the rights set out above, individuals can email us at privacy@pharmaventures.com

No fees are payable by an individual to access their personal data (or to exercise any of their rights). However, we may charge a reasonable fee if the request is clearly unfounded, repetitive or excessive.

Alternatively, we may refuse to comply with a request in these circumstances. In order to respond to a subject access request, we will need to confirm an individual's identity as a security measure to safeguard their personal data from being disclosed to non-authorised third parties. We will make all reasonable efforts to comply with an individual request within an acceptable timeframe. We are

required to respond to subject access requests where practically possible within 30 days and if this is not possible, we will provide a reasonable explanation as to why this cannot be achieved.

Complaints and queries:

If an individual is not happy with any aspect of how we collect and use data, they can contact privacy@pharmaventures.com and we will do our best to resolve the issue. Individuals can also complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk).

10. BREACHES OF THE GDPR

There is a duty on all organisations to report certain types of data breach to the relevant supervisory authority (The ICO), and in some cases to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Companies only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, the need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

The firm has implemented a Data Breach procedure.

Accurate Data:

We will make all reasonable efforts to ensure the data we hold accurate and up to date and to correct any inaccuracies that we become aware of.

Changes to this Policy

We may change this policy from time to time.

11. MONITORING & EVALUATION

This policy will be monitored and evaluated by the Data Protection Officer (or equivalent) annually and changes may be made as appropriate.

12. IMPLEMENTATION

This policy will be distributed by the Data Protection Officer or equivalent to be read and signed by all employees. Consultants will receive electronic copies to read and be required to acknowledge and confirm compliance with the contents of the policy.

13. RELATED POLICIES, PROCEDURES AND FURTHER ADVICE

If you are unsure about the contents of this policy and how it may apply to you, please speak to Adrian Dawkes the firm Data Protection Officer.

14. POLICY VERSION & HISTORY

VERSION NO.	APPROVAL DATE	APPROVED BY	AMENDMENTS MADE
0.1	February 2021	AD & EFW	New Policy
0.2	October 2025	AD & EFW	Reviewed and updated
0.3	April 2026	AD & EFW	Reviewed and updated