

Privacy Policy - Prof. Valmed®

Last Modified: September 28th, 2026

TABLE OF CONTENTS

<u>I. CONTROLLER AND CONTACT.</u>	<u>2</u>
<u>II. CATEGORIES AND SOURCES OF DATA.</u>	<u>2</u>
<u>III. PURPOSES OF PROCESSING.</u>	<u>3</u>
<u>IV. RECIPIENTS.</u>	<u>3</u>
<u>V. LEGAL GROUNDS.....</u>	<u>4</u>
<u>VI. YOUR RIGHTS.</u>	<u>4</u>
<u>VII. RETENTION.</u>	<u>4</u>
<u>VIII. AUTOMATED DECISIONS.</u>	<u>5</u>
<u>IX. COOKIES, ANALYTICS AND FONTS.....</u>	<u>5</u>
<u>X. SECURITY.....</u>	<u>5</u>
<u>XI. TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA.</u>	<u>5</u>
<u>XII. ADVERTISING AND MARKETING.</u>	<u>6</u>
<u>XIII. CORPORATE TRANSACTIONS.....</u>	<u>6</u>
<u>XIV. ANONYMOUS AGGREGATED INSIGHTS.</u>	<u>6</u>
<u>XV. CHANGES TO THIS POLICY.</u>	<u>6</u>

This Privacy Policy explains how Prof. Valmed® – validated medical information GmbH (“Prof. Valmed”, “we” or “us”) processes personal data as a controller in connection with www.profvalmed.com (the “Site”), Prof. Valmed®, Valmed A(I)cademy®, enquiries, customer relationships and professional user accounts. It also explains the distinction between those activities and processing carried out on behalf of a customer.

Where a customer, such as a healthcare organisation or professional practice, determines the purposes of processing personal data contained in queries, clinical context, Inputs or Outputs, Prof. Valmed processes that data on the customer's behalf under the applicable data processing agreement (“DPA”). The customer is responsible for providing the information required to its patients and other data subjects for that processing. This Policy does not replace the customer's privacy notice or the DPA.

“Personal data” has the meaning given in Article 4(1) of Regulation (EU) 2016/679 (“GDPR”). Information is not anonymous merely because names have been removed or several records have been combined. Pseudonymized data remains personal data.

I. CONTROLLER AND CONTACT.

For processing for which we determine the purposes and means, the controller is:

Prof. Valmed® – validated medical information GmbH
Fasanenweg 2
63225 Langen
Germany
Email: profvalmed@profvalmed.com

The competent supervisory authority for our establishment is the Hessian Commissioner for Data Protection and Freedom of Information. You may also lodge a complaint with another competent supervisory authority.

II. CATEGORIES AND SOURCES OF DATA.

Depending on your relationship with us and the features you use, we process:

- Contact and enquiry data, such as your name, organisation, professional role, email address, telephone number and the contents of your correspondence.
- Account and customer-administration data, such as your name, professional qualification or role, organisation, account identifiers, login and authentication data, subscription and billing information, and support requests. Where a customer creates or administers accounts for its personnel, we may obtain this data from that customer.
- Technical and usage data, such as IP address, device and browser information, access and security logs, timestamps, account identifiers and token counts. Whether cookie identifiers or similar data are collected depends on the technologies used on the Site; see Section IX.
- Inputs and Outputs generated when Prof. Valmed® is used. These may contain information concerning patients or other individuals, including health data. Where we process such data on a customer's behalf, its handling is governed by the DPA. Our independent processing, if any, is limited to purposes and legal grounds described in this Policy or otherwise notified where required by law.

We receive data from you, your employer or other customer that provides your access, your device when you use the Site or Service, and persons who contact us about our products. We ask customers and users to avoid direct patient identifiers unless the product instructions and contractual data protection arrangements expressly permit them.

III. PURPOSES OF PROCESSING.

As controller, we process the relevant data to:

- operate and secure the Site and Service, authenticate users, detect misuse and investigate incidents;
- establish and administer customer relationships and professional accounts, provide access to booked products and Academy modules, support users, measure use and invoice agreed fees;
- respond to enquiries and communicate service, safety and contractual information;
- comply with accounting, medical-device, security and other legal obligations, including applicable quality, vigilance and post-market surveillance requirements;
- establish, exercise or defend legal claims; and
- send marketing communications and perform optional analytics only where the applicable legal requirements are met, as further described below.

When we process patient information in Inputs or Outputs solely on behalf of a customer, the customer determines the relevant purposes and legal grounds. We process it within the documented instructions and permitted purposes under the DPA, including agreed provision, security, support, quality and regulatory processes. We do not use personal or pseudonymized Inputs and Outputs for independent model training or unrelated product development on the basis of this Policy. Any such use would require a separate valid legal basis and, where applicable, a separate agreement.

Where agreed with the customer and legally permitted, processing of personal data may be carried out to create anonymized, aggregated statistical insights. Until effective anonymization has been achieved, that processing remains subject to the GDPR, the applicable roles, documented instructions where we act as processor, and the required legal grounds. Section XIV describes the resulting anonymous information.

IV. RECIPIENTS.

Personal data may be made available, to the extent necessary for the relevant purpose, to authorised personnel; hosting, IT, support, billing and other service providers; professional advisers; and public authorities where disclosure is required or permitted by law. Providers acting on our behalf are bound by appropriate contractual and confidentiality obligations. Where we use sub-processors for customer data, the applicable DPA governs their engagement.

We do not disclose identifiable or pseudonymized patient data, individual Inputs or individual Outputs to purchasers of aggregated insights under Section XIV. Such purchasers receive only information that has been verified as anonymous under that Section and the applicable agreement.

If a customer uses an integration partner, that partner's role and access depend on the agreed integration and its own arrangements with the customer. This Policy does not determine the partner's status as controller or processor.

V. LEGAL GROUNDS.

For processing for which we are controller, the legal ground depends on the particular purpose:

- Article 6(1)(b) GDPR applies where processing is necessary to perform a contract with you personally or take steps at your request before such a contract. Where your organisation is the contracting party, account administration and communication with you may instead rely on Article 6(1)(f) GDPR, subject to a balancing of interests.
- Article 6(1)(f) GDPR may apply to necessary Site and Service security, fraud prevention, customer communication, support, service administration, proportionate technical diagnostics and legal claims. Our interests are in maintaining a secure, functional professional service and protecting our business and users. You may object on grounds relating to your particular situation.
- Article 6(1)(c) GDPR applies where processing is necessary to comply with a legal obligation, including applicable tax, accounting and medical-device duties.
- Article 6(1)(a) GDPR applies where we request valid consent, including for optional technologies or marketing where consent is required. Consent can be withdrawn at any time with effect for the future.

For any independent processing by us of health data, an applicable condition under Article 9(2) GDPR is required in addition to an Article 6 legal ground. The particular condition depends on the purpose and relevant law; this Policy does not establish a general right to use patient health data for our own commercial purposes. Where we act as processor, the customer or other controller is responsible for determining its Article 6 legal ground and, where health data is involved, an applicable Article 9 condition, including for any instructed anonymization.

VI. YOUR RIGHTS.

For personal data for which we are controller, and subject to the conditions and limits in the GDPR, you may request access, rectification, erasure, restriction of processing or data portability; object to processing based on Article 6(1)(f); and withdraw consent at any time without affecting processing that was lawful before withdrawal. You may lodge a complaint with a supervisory authority.

You can exercise your rights by writing to profvalmed@profvalmed.com. Where your request concerns data that we process on behalf of a customer, we will direct you to the relevant controller or assist that controller under the DPA, as appropriate.

VII. RETENTION.

We retain personal data only for as long as needed for the purposes described here, subject to applicable legal retention duties. The applicable period depends on the category of data and purpose. For example, account data is generally retained for the customer relationship and a necessary period thereafter for contractual and legal claims; invoices and accounting records are retained for the period required by law; security logs are retained for the period necessary to detect and investigate incidents. We delete or anonymize data when the applicable purpose and retention obligation end.

Retention and return or deletion of personal data in Inputs and Outputs processed on behalf of a customer are governed by the applicable DPA and any overriding legal or medical-device obligations. This Policy does not impose a general 36-month retention period on such Content. Once information has been lawfully and effectively anonymized, it is no longer personal data; see Section XIV.

VIII. AUTOMATED DECISIONS.

We do not make decisions about website visitors, customers or users based solely on automated processing that produce legal or similarly significant effects within the meaning of Article 22 GDPR. Prof. Valmed® provides decision support to qualified healthcare professionals; clinical decisions remain with the responsible professional in accordance with the applicable Instructions for Use.

IX. COOKIES, ANALYTICS AND FONTS.

The Site may use cookies and comparable technologies. Technologies strictly necessary to transmit communications or provide a service expressly requested by you may be used without a separate consent under applicable law. We obtain consent before using optional technologies where required by Section 25 of the German Telecommunications Digital Services Data Protection Act (TDDDG) and the GDPR. Any consent can be withdrawn with effect for the future.

Session cookies are generally deleted when the browser session ends. Other cookies may remain for a defined period or until you delete them. Browser settings can restrict cookies, although necessary functions may then be unavailable. The actual providers, purposes and lifetimes of optional technologies must be stated in the Site's cookie information and consent interface where such technologies are used.

We use analytics technology based on Snowplow to understand use of the Site. Depending on its configuration, technical identifiers and usage events may be personal data; we do not classify all such data as anonymous merely because it is used for statistics. If this technology accesses information on your device beyond what is strictly necessary, we use it only after obtaining any required consent. We use the resulting personal data only for the purposes and periods disclosed for the configured technology.

The Site may use Google Web Fonts. Where fonts are loaded from Google's servers, your browser may transmit technical data such as your IP address to Google. Where fonts are hosted locally, no such request is made to Google for the fonts. The actual implementation and any required consent or transfer safeguard must be reflected in the Site's technology information.

X. SECURITY.

We implement appropriate technical and organisational measures, taking into account the nature of the data and risks, to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Access is restricted to authorised persons with a relevant need.

XI. TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA.

Where personal data is transferred to a recipient outside the European Economic Area, we use a lawful transfer mechanism where required, such as an adequacy decision or appropriate safeguards including the European Commission's standard contractual clauses, together with supplementary measures where necessary. Information about applicable safeguards may be requested using the contact details above. Transfers by sub-processors for customer data are also subject to the applicable DPA.

XII. ADVERTISING AND MARKETING.

If we use third-party advertising technologies or optional tracking to present or measure advertisements, we will identify the technologies and obtain prior consent where required. We do not rely on this Policy alone as consent to install advertising cookies or to disclose personal data to advertising providers.

We may contact you about our products and services where permitted by applicable law. Where consent is required, we obtain it separately. You may withdraw consent or object to direct marketing at any time, for example through an unsubscribe function or by contacting us. Service, safety and necessary account communications are not marketing messages.

XIII. CORPORATE TRANSACTIONS.

If our business or relevant assets are transferred, personal data may be disclosed to prospective or actual acquirers to the extent lawfully necessary, subject to appropriate confidentiality and data protection safeguards. We will provide further information where required by law. A transaction does not itself expand the purposes for which customer data may be used under a DPA.

XIV. ANONYMOUS AGGREGATED INSIGHTS.

Where lawfully permitted and agreed with the relevant customer, we may process Service data to create aggregated statistical data, trends and signals. If the source data is personal data processed on a customer's behalf, the creation of these insights requires the appropriate documented instruction or other valid arrangement and a lawful basis for the underlying processing, including any applicable Article 9 condition. The processing remains subject to the GDPR until the resulting information is effectively anonymous.

We assess the result against reasonably likely means of identification, including singling out, linkage and inference, and apply appropriate controls such as suppression or generalisation of small or rare groups. Only after effective anonymization has been documented may we use, combine, disclose, license or sell the anonymous aggregated insights to third parties for analytics, research, market research or industry intelligence, in accordance with the applicable customer agreement. These insights must not identify a patient, individual user, customer or healthcare organisation or reproduce an individual Input or Output. We do not sell personal data or pseudonymized data under this arrangement.

XV. CHANGES TO THIS POLICY.

We may update this Policy to reflect changes in our processing or legal requirements. We will publish the updated version with its effective date and provide additional notice where required by law. A change to this Policy does not by itself amend a customer's agreement or DPA. Continued use of the Site or Service is not treated as consent to a new purpose that requires consent.

Contact

For privacy questions or requests, contact profvalmed@profvalmed.com or write to Prof. Valmed® – validated medical information GmbH, Fasanenweg 2, 63225 Langen, Germany.