PRIVACY STATEMENT version 2.0

ZEUS SOFT srl

Rue Jean Sonet 25

B – 5032 Isnes

Tax ID: BE0647.962.374

PRIVACY STATEMENT

In compliance with GDPR legislation (in force since 25/5/2018)

1. WHAT IS THIS STATEMENT?

It explains how we handle your personal data, what your rights are and how you can exercise them.

Terms used:

- **Personal data**: by this the GDPR means all information that could directly or indirectly identify a natural person. Further, referred to as "data." So it is NOT about company data.
- **Processing**: collecting, recording, organizing, structuring, storing, updating or modifying, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying data.

2. WHAT TYPE OF DATA DO WE PROCESS?

We process the following personal data about you:

As Controller;

- **Contact Details which may include sex, name, email, address, phone number, preferred contact method, job title, company name, any data relative to purchases and product usage.**
- **Personal details of our authors/collaborators/partners which may include sex, birth date, college degree and awards, interest groups and affiliations with other associations, as well as the abovementioned data.**

As Processor or third party provider;

- **Sensitive personal data and more specifically patient data, managed by our customers. Sensitive data is normally encrypted and may only become visible under specific circumstances (like technical servicing upon agreement of the owner of such data).**

How data has come to us:

- By registering and logging in to one of our applications:

  https://www.radaropus.com

  https://www.crm.zeus-soft.com

  https://www.clificol.net

  https://www.opus.plus

  https://opusgo.app/register

We do not collect data in any other way.

3.PURPOSE:

In the context of the global processing of personal data, and in compliance with the General Data Protection Regulation (GDPR) as well as applicable privacy laws in other jurisdictions, we process customers' personal data solely for the purpose of facilitating the ordering and delivery of products and documents specifically related to homeopathy, naturopathy and/or associated to healthcare services. This processing is necessary to fulfill contractual obligations, including the handling of orders or support requests placed by our customers, and to enhance communication and customer support. All data processing activities are carried out in accordance with the highest standards of data security and confidentiality, regardless of the customer's geographical location.

4.STORAGE and SANITIZATION:

We will keep your data for as long as you use our applications or software and for as long as we need your personal data to be able to offer you our services.

In particular:

- We retain accounting records for a minimum period of 7 years, either in original or electronic form. The retention period begins on 1 January of the year following the end of the relevant financial year. Our retention practices comply with applicable local and international accounting regulations, ensuring compliance with the legal requirements of each country in which we operate.
- Additionally, we retain personal data for the duration of the business relationship. Upon termination of the relationship, personal data will be securely deleted after a retention period of 7 years, unless otherwise required by applicable law or regulatory obligations or unless necessary to guarantee you our services.
- We have a formal destruction procedure in place for all records, including accounting and personal data. This procedure ensures that records are securely destroyed once the legal retention periods have expired, in accordance with applicable laws and regulations. The destruction process is designed to prevent unauthorized access, use, or disclosure of the data, ensuring full compliance with data protection and privacy standards.
- In compliance with the EU General Data Protection Regulation (GDPR), we retain personal data of employees for a period of 5 years following the termination of employment. After this period, the data will be securely deleted unless otherwise required by applicable law or necessary to guarantee services to our company and/or to our customers.
- Processing of Personal Data by Our Partners for Whom We Provide Services as a Third-Party Provider.
  When using our applications, data controllers such as doctors, homeopaths, and other healthcare providers may process personal and sensitive data, including health information.

These partners act as data controllers within the meaning of the General Data Protection Regulation (GDPR) and are independently responsible for compliance with the relevant data protection laws and regulations.

Responsibility of Our Partners:

When partners, such as doctors, homeopaths, healthcare professionals or similar, use our applications to store and process personal data, we do not have access to such data and they act as independent data controllers. These partners are responsible for ensuring compliance with the applicable laws, such as the GDPR, and must take the necessary technical and organizational measures to safeguard the security and confidentiality of the data.

If you have provided personal or sensitive data to one of our partners through our applications, we advise you to contact the respective party directly to exercise your rights under the GDPR. This includes, but is not limited to, the right to access, rectification, restriction of processing, data portability, and the right to request erasure of your data. Please note that we, as the provider of the application, act as a data processor and do not have control over the processing of this data, and are therefore not responsible for the compliance of our partners with data protection regulations.

We enter into data processing agreements with all of our partners, such as doctors, homeopaths, and other healthcare providers, in which they declare that they will at all times comply with the General Data Protection Regulation (GDPR) and other applicable data protection laws in the country where they are established. These agreements set out the responsibilities of the partners with regard to compliance with the relevant data protection rules and ensuring appropriate security measures for the processing of personal data.

If partners process personal data of individuals residing outside their own jurisdiction, they are obligated, under these data processing agreements, to also comply with the applicable laws and regulations of the countries where these individuals reside. This means that, in addition to complying with local regulations, the processing must also adhere to the data protection rules that apply in the jurisdiction of the individuals concerned, including but not limited to the GDPR, where applicable.

5.SECURITY:

For this processing, we take the **appropriate technical and organizational** measures to optimally protect your data, taking into account the nature of the data and the associated risks. We do not store any special personal data and have the following measures in place for the security of your data:

- The computers on which data are processed are protected by default with a username and a complex password.
- All computers are equipped with a Small Office Security solution, which is of course always kept "up-to-date" and automatically performs multiple scans. All PC installations are automatically updated. The installation is checked at least once a month and started manually if necessary.
- All personal data is securely stored in our own infrastructure, which includes a self-installed NAS, an internally hosted CRM, an external encrypted CRM, and through Microsoft Office 365 services. Our data storage solutions are entirely under our control, ensuring that all personal information is stored locally, without reliance on third-party cloud providers. By

hosting our own CRM system and managing our own databases, we minimize external access and maintain complete ownership over the data we process.

- We take the necessary measures to ensure both digital and physical security of personal data. Access to digital systems is protected by password security, and/or two-factor authentication (2FA). Additionally, physical documents are secured in locked cabinets to prevent unauthorized access. For certain systems, such as Office 365, we ensure data access is protected according to Microsoft's security protocols, but we continuously monitor and verify our own security measures internally.
- We do not transfer personal data to any external companies or cloud services outside the EU without meeting the required conditions and obligations under the General Data Protection Regulation (GDPR). This includes compliance with Articles 13.1(e), 14.1(f), 15.2, 30.1(e), and Articles 44-50. Any necessary cross-border data transfers are conducted in full accordance with data protection regulations. In the event personal data is shared, such as with a company that requires updates, corrections will be communicated to the receiving party to ensure accuracy and compliance.
- Please note that while we utilize Microsoft 365 services, we do not have direct control over the specific servers Microsoft may use to process this data. When personal data is processed through services like Office 365, Microsoft may leverage its global data centers to optimize performance based on the user's location, in compliance with applicable data residency requirements.
- We collect and retain personal data strictly for specified, explicit, and legitimate purposes. This includes maintaining contact with our customers, keeping them informed about product updates, ensuring the security and compatibility of our software, and preventing piracy or unauthorized access. For example, during remote support sessions, we may verify customer information such as account details to ensure that the individual seeking support is the registered user.
- All passwords are securely managed and stored using a cloud-based password management system, which encrypts all credentials and ensures that they are only accessible to authorized users through multi-factor authentication.
- Our employees are fully informed about the safe handling of your personal data and are bound by their employment contract to confidentiality.

Past experience teaches us that no risk is completely avoided and should we become aware of any unauthorized access to our IT systems or unlawful alteration, damage or possible loss of your data, we will immediately take **all necessary measures** to minimize this risk and avoid it in the future. As a result, the possible damage to you will also be very limited.

6. MARKETING PURPOSES.

CLICK BEHAVIOUR AND VISIT DATA

General visitor data is kept on our company's website. In this context, the IP address of your computer, any user name, the time of retrieval and data sent along with a visitor's browser may be recorded and used for statistical analyses of visitor and click behavior on the website and our

products/services. We also use this to optimize the operation of our website and products/services. We try to anonymize this data as much as possible. This data will never be provided to third parties unless specifically requested in writing by us and granted by you.

WEBSITE ANALYTICS

Our website's landing page uses Google Analytics (or similar) to track how visitors interact with our site and to measure the effectiveness of our Google Ads campaigns on search result pages. The data collected through Google Analytics, including your computer's IP address, may be transferred to and stored by Google on servers located in Dublin. For more information, please refer to Matomo's privacy policy (https://matomo.org/)

We have taken steps to ensure that Matomo is only used on our landing page, and no data is tracked or collected through the app. Additionally, Matomo will not use the analytics information collected for other services unless required by law or if third parties process the data on Matomo's behalf. We have ensured that any data collected is in compliance with the GDPR and other applicable global privacy regulations.

LINKEDIN and YOUTUBE

Our website includes buttons to promote or share content via Social Media applications such as Facebook, LinkedIn and YouTube. These buttons are implemented using code provided by the respective social media platforms, which may set cookies on your device (see our cookie policy for more details).

Please review the privacy policies of these Social Media platforms to understand how they handle your personal data, as we have no control over how these platforms process your data through the embedded buttons and cookies. Their privacy policies may change periodically, and we encourage you to stay informed.

We ensure that our use of these social media integrations complies with applicable global data protection regulations, including GDPR. However, we advise users to review the privacy policies of these platforms and make informed decisions regarding the use of their services on our website.

NEWSLETTER

We offer a newsletter with which we want to inform interested parties about news, our services and related matters. Your email address will only be added to the list of subscribers with your explicit consent. Each newsletter contains a link with which you can unsubscribe. The subscriber base of the newsletter will not be passed on to third parties.

CONTACT

When you fill in any type of form on one of our platforms, like our website, your personal data will be processed as described in this privacy statement. You can always contact us by email for any queries to info@zeus-soft.com , dpo@zeus-soft.com or info@dpoassociates.eu

USE OF COOKIES

We use cookies when offering electronic services. A cookie is a simple small file that is sent along with pages of this website and stored by your browser on your computer's hard drive. We use cookies to remember your settings and preferences if you click on them for approval. According to privacy-by-design, the analytical cookies are set to off by default. You can also disable these cookies through your browser.

For more information, please consult our **Cookie Statement** .

7. **Data Sharing and Processing:**

Use of Mailchimp for Marketing Communications

We use Mailchimp, a third-party service provider, to manage and send our marketing campaigns and email communications. Mailchimp is a product of The Rocket Science Group LLC, based in the United States. By subscribing to our newsletter or other marketing-related communications, you agree that your personal data (such as your email address and name) will be processed by Mailchimp in accordance with their privacy policy.

- https://mailchimp.com/legal/privacy/

Purpose of Data Processing:

The data we collect through Mailchimp is used solely to inform you about our products, services, promotions, and other relevant information. We process this data based on your explicit consent (as required under Article 6(1)(a) of the General Data Protection Regulation, GDPR).

Security and Data Protection:

Mailchimp complies with applicable European data protection regulations, including the General Data Protection Regulation (GDPR). Mailchimp has implemented appropriate technical and organizational measures to ensure the security of your personal data. In addition, Mailchimp is certified under the EU-U.S. Data Privacy Framework, providing an adequate level of protection for data transfers to the United States.

You can unsubscribe from our marketing communications at any time by using the unsubscribe link provided in each email we send via Mailchimp. Additionally, you can request access to, correction, or deletion of your personal data processed through Mailchimp. For further information on how Mailchimp processes data, please refer to their privacy policy at Mailchimp Privacy Policy.

8. **YOUR RIGHTS**

Below is a list of your rights regarding the processing of your personal data, applicable under different global data protection regulations. These rights may vary depending on the jurisdiction in which you reside, but we aim to comply with relevant laws worldwide, including the **EU General Data Protection Regulation (GDPR)**, **California Consumer Privacy Act (CCPA)**, and other international privacy frameworks.

1. **Right of Access**
   You have the right to request access to the personal data we hold about you. If there are errors or omissions in the data, you may request corrections, additions, or deletions where applicable under the law.
   EU GDPR: Articles 12-13-14
   Other jurisdictions: Access rights may vary depending on local laws.
2. **Right to Rectification**
   You have the right to have your personal data corrected if it is inaccurate or incomplete.
   EU GDPR: Article 16
   CCPA: You have the right to request the correction of inaccurate personal information.
3. **Right to Erasure ("Right to be Forgotten")**
   You can request the deletion of your personal data if it is no longer needed for the purposes outlined in this privacy statement or if there is no longer a legal basis for retaining it.
   Note: Deletion may be restricted where data must be retained for compliance with legal obligations, such as tax and social security legislation.
   EU GDPR: Article 17
   Other jurisdictions: Rights to deletion may vary depending on local regulations.
4. **Right to Data Portability**
   If you wish to switch service providers, we will provide your personal data in a structured, commonly used, and machine-readable format, so it can be transferred to the new provider.
   EU GDPR: Article 20
   Other jurisdictions: Portability rights may not be explicitly defined outside the EU but can still be honored if requested.
5. **Right to Object to Processing**
   In certain circumstances, you have the right to object to the processing of your personal data, particularly if it is used for direct marketing purposes. However, we do not process personal data for marketing purposes, so this right is not applicable in our case.
   EU GDPR: Article 21
   CCPA: You have the right to opt out of the sale of your personal information.
6. **Right to Restrict Processing**
   In some cases, you may have the right to request that we restrict the processing of your personal data if certain conditions are met, such as if you dispute the accuracy of the data or if the processing is unlawful but you oppose deletion.
   EU GDPR: Article 18
   Other jurisdictions: Similar rights may exist under local regulations, though restrictions on processing may differ.
7. **Right to Transparency**
   You have the right to be informed about the processing of your personal data. This privacy statement is available via this link, attached to all electronic communications, and visibly posted in our offices.
   EU GDPR: Article 12
   Other jurisdictions: Transparency obligations vary globally, but we aim to keep you fully informed about how we handle your data.

8. **Right to Complain to a Supervisory Authority**
   If you believe that your data protection rights have been violated, you have the right to lodge a complaint with a relevant supervisory authority.
   EU GDPR: Article 77
   Other jurisdictions: You may have the right to file complaints with local authorities depending on the laws in your country.

How to Exercise Your Rights

If you wish to exercise one or more of the rights listed above, please submit your request in writing, along with proof of your double Opt-In verification by email. We will respond to your request within 30 days, in accordance with applicable data protection regulations.

9. COMPLAINTS

If you disagree with the way we handle your personal data, how we respect your rights, or with any part of this privacy statement, we encourage you to contact us first, so that we can address your concerns promptly and appropriately.

If you are not satisfied with our response, or if you believe that your personal data is being processed in violation of applicable data protection laws, you have the right to file a complaint with the relevant data protection authority in your country or region. Depending on where you are located, you can contact one of the following authorities:

- **For individuals within the European Union (EU)**: You may file a complaint with the data protection authority in your country. For example, in Belgium, this is the **Data Protection Authority (DPA)**, which can be reached via www.gegevensbeschermingsautoriteit.be, located at 1000 Brussels, Drukpersstraat 35, or via email at contact@apd-gba.be or by telephone at +32 2 274 48 00.
- **For individuals in other countries**: Please consult your local data protection authority to file a complaint. We comply with the applicable data protection regulations of each region, including but not limited to the GDPR, CCPA, and other international laws.

We are committed to handling all complaints in accordance with the relevant data protection laws of your country, and we will work to resolve any issues in a timely and transparent manner.

10. MISCELLANEOUS:

This updated privacy statement will enter into force on 12 February 2025.

We reserve the right to change this privacy statement at any time.

11. CONTACTS REGARDING THIS PRIVACY STATEMENT:

If you have questions after reading this statement, please contact our Data Protection Officer (DPO), Mr. Danny Baerts **at** dpo@zeus-soft.com or info@DPOassociates.eu