PRIVACY NOTICE

Last updated 16th May. Version 2.0

This privacy notice for Oomph Works Ltd ("**Company**," "**we**," "**us**," or "**our**"), describes how and why we might collect, store, use, and/or share ("**process**") your information when you use our services ("**Services**"), such as when you:
Questions or concerns? Reading this privacy notice will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact us at hello@oomphworks.com.

SUMMARY OF KEY POINTS

This summary provides key points from our privacy notice, but you can find out more details about any of these topics by clicking the link following each key point or by using our table of contents below to find the section you are looking for.

What personal information do we process? When you visit, use, or navigate our Services, we may process personal information depending on how you interact with Oomph Works and the Services we provide, the choices you make, and the products and features you use.

Do we process any sensitive personal information? We do not process sensitive personal information.

Do we receive any information from third parties? We may receive information from public databases, marketing partners, social media platforms, and other outside sources.

How do we process your information? We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so.

In what situations and with which parties do we share personal information? We may share information in specific situations and with specific third parties. Learn more about

What are your rights? Depending on where you are located geographically, the applicable privacy law may mean you have certain rights regarding your personal information.

How do you exercise your rights? The easiest way to exercise your rights is by submitting a data subject access request, or by contacting us. We will consider and act upon any request in accordance with applicable data protection laws.

Want to learn more about what Oomph Works Ltd does with any information we collect?

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE COLLECT?

Personal information you disclose to us

In Short: *We collect personal information that you provide to us.*

We collect personal information that you voluntarily provide to us when you register on the Services, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

Sensitive Information. We do not process sensitive information.

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information.

Information automatically collected

In Short: *Some information — such as your Internet Protocol (IP) address and/or browser and device characteristics — is collected automatically when you visit our Services.*

We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Services, and other technical information. This information is primarily needed to maintain the security and operation of our Services, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies.

2. HOW DO WE PROCESS YOUR INFORMATION?

In Short: *We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.*

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

3. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

In Short: *We may share information in specific situations described in this section and/or with the following third parties.*

We may need to share your personal information in the following situations:

- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us.

- **Business Partners.** We may share your information with our business partners to enable certain products and services. .

4. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

In Short: *We may use cookies and other tracking technologies to collect and store your information.*

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice.

5. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

In Short: *We may transfer, store, and process your information in countries other than your own.*

Our servers are located in the United Kingdom. If you are accessing our Services from outside, please be aware that your information may be transferred to, stored, and processed by us in our facilities and by those third parties with whom we may share your personal information (see "WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?" above), in and other countries.

If you are a resident in the European Economic Area (EEA) or United Kingdom (UK), then these countries may not necessarily have data protection laws or other similar laws as comprehensive as those in your country. However, we will take all necessary measures to protect your personal information in accordance with this privacy notice and applicable law.

6. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: *We keep your information for as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements).

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because

your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

7. DO WE COLLECT INFORMATION FROM MINORS?

In Short: *We do not knowingly collect data from or market to children under 18 years of age.*

We do not knowingly solicit data from or market to children under 18 years of age. By using the Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact us at hello@oomphworks.com.

8. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: *You may review, change, or terminate your account at any time.*

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your Member State data protection authority or UK data protection authority.

If you are located in Switzerland, you may contact the Federal Data Protection and Information Commissioner.

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us by using the contact details provided in the section "HOW CAN YOU CONTACT US ABOUT THIS NOTICE?" below.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:
Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

9. CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this privacy notice.

10. DO CALIFORNIA RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: *Yes, if you are a resident of California, you are granted specific rights regarding access to your personal information.*

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information provided below.

If you are under 18 years of age, reside in California, and have a registered account with Services, you have the right to request removal of unwanted data that you publicly post on the Services. To request removal of such data, please contact us using the contact information provided below and include the email address associated with your account and a statement that you reside in California. We will make sure the data is not publicly displayed on the Services, but please be aware that the data may not be completely or comprehensively removed from all our systems (e.g., backups, etc.).

11. DO WE MAKE UPDATES TO THIS NOTICE?

In Short: *Yes, we will update this notice as necessary to stay compliant with relevant laws.*

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information.

12. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, you may email us at hello@oomphworks.com or by post to:

Oomph Works Ltd
1 The Gateway
Silkwood Park
Wakefield, West Yorkshire WF5 9TJ
United Kingdom
Phone: 01924 926414

13. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?

Based on the applicable laws of your country, you may have the right to request access to the personal information we collect from you, change that information, or delete it. To request to review, update, or delete your personal information, request a data access request by emailing hello@oomphworks.com

14. WHAT MECHANISMS WE HAVE IN PLACE FOR SENSITIVE DATA.

Access Controls: role-based access controls (RBAC) to ensure that only authorized personnel have access to sensitive customer data. Administrators have defined roles with specific access privileges based on job responsibilities.

Encryption: Encrypt sensitive data stored in the database to protect it from unauthorized access. Encryption techniques can be applied to fields containing sensitive information such as passwords and payment details. Additionally, ensure that data transmitted between the software and system and other applications or users is encrypted using secure protocols.

Anonymization and Pseudonymization: Anonymize or pseudonymize sensitive data to protect customer privacy while still allowing for analysis and reporting. For example, replace customer names and contact details with unique identifiers or pseudonyms in analytical reports to prevent the identification of individuals.

Audit Trails: Implement audit trails to track user activity within the system. Record details such as user logins, data access, modifications, and exports. Audit logs help identify unauthorized access or suspicious behaviour and provide accountability for data handling.

Data Masking: Mask sensitive data fields in the software user interface to prevent unauthorized viewing by employees who do not require access to that information.

Two-Factor Authentication (2FA): Enhance security by requiring users to authenticate with an additional factor, such as a one-time passcode sent to their email, in addition to their username and password. 2FA adds an extra layer of protection against unauthorized access, especially for accounts with access to sensitive data.

Data Retention Policies: Established data retention policies to govern the storage and deletion of sensitive customer data in the system. Clear guidelines for how long different types of data should be retained based on regulatory requirements and business needs. Ensure that expired data is securely deleted from the system to minimize the risk of data breaches.

Regular Security Assessments: Regular security assessments and vulnerability scans to identify and address potential weaknesses in the systems are conducted. Any security vulnerabilities are patched promptly and update security measures as needed to protect against emerging threats.