

Privacy Policy

In brief: We are ChefPro L S, LTDA. ("ChefPro," "we" or "us"). We respect your privacy and work hard to protect the confidentiality of information that you give us. We will share your personal data with third parties only in the event that it's needed for the provision of services and data you have requested (explained in detail in this privacy policy).

About Us

ChefPro is the data controller responsible for your personal data and is the sole owner of the chefproapp.com website ("Website"), ChefPro mobile and desktop applications, ChefPro services (each, a "Service") and all of the information collected on it. ChefPro collects information from users in several ways (explained in detail in this privacy policy).

This privacy policy applies to personal data that we collect from you when you visit this Website, create an account, use our applications or services ("you" or "your" being interpreted accordingly). It provides information on what personal data we collect, why we collect personal data, how it is used, the lawful basis on which your personal data is processed, how it is stored, and how we share information.

As used in this privacy policy, "personal data" means any information that relates to you from which you can be identified.

By using our Service or submitting your personal data, you are agreeing to accept the terms of this privacy policy, so please read it carefully. If you

disagree with this privacy policy at any point or time, you should stop using our Services and delete your user account.

Updates

We may update this privacy policy at our discretion from time to time by posting a new version on our Website. You should check our Website occasionally to ensure any changes made are suitable for you. If required by applicable law, you will be informed of any significant changes made to the privacy policy.

The current version of this privacy policy was modified on April 22, 2021.

Personal data that we collect

Data we receive from you

User Accounts

If you decide to create an account, you will need to provide us with some personal data so we can provide you with access to our additional services that users benefit from. You may also elect to provide us with additional information about you, as described below.

During registration you will be required to provide us with either:

- your username, email address;
- your account information with one of the following social Internet services: Facebook, Google; and
- if you want to buy a subscription, we will need your first name and last name.

In some cases, you may need to provide and verify your phone number. You can also add additional information about yourself in the profile settings, however, this is not mandatory.

The following information will not be publicly displayed:

- your first and last name, phone number, email, company, address.

If you register to be a user of Basic/Professional/Pro+Nutri (a "**Paid User**"), our third party payment processor will also process information about your payment card and bank account information or payment account information that we require for the purpose of recording and processing your account registration. For further details, please refer to the point below titled "Plans", in website and app side menu.

Contact data

We also process any personal data you choose to give when corresponding with us by email, or otherwise visiting and interacting with this Website or any other services we operate.

Cookies and other technologies

We use browser cookies (small text files placed on your device) to administer our Site, gather and analyze statistical information, ensure security, to fight spam, and for advertising purposes. Cookies allow us to provide you with a better user experience when you browse our Website and helps to improve its features. More detailed information on the use of cookies can be found in our Cookies Policy.

We also use web beacons (tiny graphics with a unique identifier) for analytics and advertising purposes and to develop, test, and improve our services further, as described in our Cookies Policy.

Log files

Like most websites, we use web server log files. Records in our log files include internet protocol (IP) addresses (see the "Device information" section below for further details), browser types, internet service providers, referring pages, exit

pages, platform types, and date/time stamps. We use web server log files to administer the site, provide broad traffic information for site planning purposes, and to ensure that our terms of service agreement is being adhered to. Note that IP addresses are not tied to personal data in our web server log files.

Device information

We collect the following information about the devices you use to interact with our services: IP address of the device (from which we can also infer the country you are connecting from), operating system, and browser version. We collect this information to prevent spam and abuse of our services. IP addresses may be considered personal data in certain jurisdictions, and will be treated in accordance with this privacy policy.

Analytics

When you are using our Website, mobile and desktop applications, or widgets we provide to another site, we may collect analytics information automatically. This information may include your general device information, device identifiers (for example, Google Advertising ID, if you are using an Android device, or Advertising Identifier (IDFA), if you are using an iOS device), network information, website, and application interaction events. We collect pseudonymous data only and this analytic information does not include any personal identifiable information from your profile. We use this information to analyze and improve the work of our services and applications, and to develop, test, and improve our service further. For this purpose we may use internal analytic as well as third party service providers. For further details about our use of third party service providers, please refer to the Analytics providers section below.

Data we receive from third parties

When you sign in to your account using your social internet service credentials (Facebook, Twitter, Google, Yahoo!, LinkedIn), such service sends us your username and the email address associated with the credentials you've used. We neither control nor take any responsibility for the way third parties provide information about you and/or process your personal data.

How personal information is used

We use personal data in various ways that are necessary to provide the services you intend to use, certain legitimate interests, and as a necessity in order to comply with applicable law, as further described below.

We do not generally rely on your consent to allow us to process your personal data if there is another lawful ground available. If we do rely on your consent, we will make this clear to you at that time.

Profile

A profile is a set of information for each individual user that details his/her viewing preferences. User settings (chart settings, toolbars, buttons, etc.) are kept solely for the purpose of customizing the user's experience when using the Website, applications or user accounts. We do not share private profile settings with any third parties.

Note that when you create an account, other users or visitors may access your public profile and see any information you have made publicly available about yourself.

User account and profile operations

We use your contact details, such as username, email address, or phone number, in the following ways:

- to authenticate your user account, ensure its security along with the security of our services, and to prevent spam, fraud, and abuse;
- to acknowledge, confirm, and deal with your user account;
- to send all new users a welcome activation email to verify their email address;
- (For Paid Users) to provide you with subscription services and contact you regarding your use of such services. This is necessary for us to implement your requests; and

- Paid Users will also receive a notification email from PayPal if there are any issues regarding billing their cards for auto-renew subscriptions. Users cannot opt out of these messages, though they can delete their account.

User account deleting

You may refuse to use our Website and/or application and may ask us to delete your account in the Profile settings. Your account will be deleted after 30 days. During this time, you can stop the deletion process at any time.

Please note that if you have requested your account to be deleted, we will delete the subsequent personal data you have supplied us. Note that search engines, as well as third parties, can keep copies of your publicly available information once your account has been deleted. It should also be noted that published ideas will remain on the site and messages sent to other users cannot be deleted.

Marketing

We may send you marketing emails about our products or services that are similar to the products or services you are subscribed to, including information about events and other promotions we feel may interest you. This is unless you have indicated to us that you do not wish to receive communications in this manner. We will send you other promotional information by email only with your consent, which was given at the time you provided us with your personal data. Users can opt out of receiving marketing communications at any time by clicking "unsubscribe" in one of the emails (for more information on your rights, please see the "User rights" section below).

Service-Related Announcements

On rare occasions, it may be necessary to send out service-related announcements. For instance, if our service is interrupted for a prolonged period or a major functionality upgrade is released, we might send all users an email message.

Customer Service

When you open a support ticket, we use your contact details as well as information about your device, server logs, a description of the problem, along with any other supporting materials (videos, screenshots, etc.) to help resolve the issue(s).

Legitimate interests

We will process your personal data as necessary for certain legitimate business interests, which include the following:

- where we are asked to respond to any of your inquiries, comments, or grievances;
- to administer our services in order to better understand how visitors interact with the Website and application, and ensure that they are presented in the most effective manner for you and your computer/device;
- to develop and improve our mobile applications;
- to share personal data among our affiliated businesses for administrative purposes, provide subscription services, and in relation to our sales and marketing activities, except where we require your consent, as described above;
- to send you information about our products or services that are similar to the products or services you subscribed to (unless you have refused or opted out of receiving these emails at the time you provided us with your email address or you have indicated to us that you do not wish to receive communications in this manner). Our legitimate interest is to ensure our marketing is relevant to you, so we may process your data to send you information on our products or services that is specifically tailored to your interests;
- we may anonymize, pseudonymize, aggregate and de-identify the data that we collect and use this data for our own internal business purposes, including sharing it with our business partners, our affiliated businesses, agents and other third parties for commercial, statistical and market research purposes. For example, to allow those parties to analyze

patterns among groups of people and conducting research on demographics, interests, and behavior;

- for internal business/technical operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes, and as part of our efforts to keep our Website, network, and information systems secure; and
- to (a) comply with legal obligations, (b) respond to requests from competent authorities; (c) enforce our Terms of Use or House Rules; (d) protect our operations or those of any of our affiliated businesses; (e) protect our rights, safety or property, and/or that of our affiliated businesses, you or others; and (f) enforce or defend legal rights, or prevent damage. This means we can store and disclose your information to law enforcement authorities, state, or government agencies if we establish that such disclosure is necessary to comply with the law. This includes responses to court orders or subpoenas, as well as other judicial or regulatory processes.

As used in this privacy policy, “legitimate interests” means the interests of ChefPro and our affiliated businesses in conducting and managing our business. When we process your personal data for our legitimate interests, we make sure to consider and balance any potential impact on you and your rights under data protection laws. Our legitimate interests do not automatically override your interests. We do not use personal data for activities where our interests override the impact they may have on our users, unless we have their explicit consent or those activities are otherwise required or permitted by law. You have the right to object to the processing of your personal data that is based on our legitimate interests at any time, on grounds relating to your particular situation (for more information on your rights, please see the "User rights" section below).

When would we share personal information

We share your personal data with third parties in the following situations:

- **Service providers:** ChefPro, like many businesses, occasionally engages with selected third parties who act on our behalf to support our operations, such as (i) card processing or payment services (see the point below headed "Payment information"), (ii) IT suppliers and contractors (i.e. data hosting providers or delivery partners) as necessary to provide IT support and enable us to provide subscription services and other goods/services available on this Website or to users, (iii) web and mobile analytics providers, (iv) providers of digital advertising services, and (v) providers of marketing and sales software solutions. Pursuant to our instructions, these parties may access, process or store your personal data in the course of performing their duties to us and solely in order to perform the services we have hired them to provide.
- **Payment information:** Paid Users must provide payment information (name, payment card information or payment account information). This information is used for billing purposes only and is processed by our payment processors. When you are making a payment, we do not have access to your payment card information. Should we have any issues with processing an order, the email address you have provided will be used to contact you.
- **ChefPro affiliated businesses:** In order to provide the services you request from us, our affiliated businesses may access and process the information which we collect from you for the purposes described above, including offering products and services to you. Our affiliated businesses will only use your data for the purposes for which we originally collected said data.
- **Analytics providers:** We may use third-party service providers to monitor and analyze the use of our services and mobile applications. We use this information to analyze and improve the work of our services and mobile applications.
 - We may use Google Analytics as a web analytics service on the Website and in conjunction with the widgets we provide. For

more information on Google Analytics privacy practices, you can check [here](#).

- Analytics services for mobile applications that we may use:
 - Firebase – a development and analytics platform provided by Google. For more information on what type of information is collected, please visit the [Google Privacy web page](#).
 - Flurry Analytics – provides us with tools and resources for understanding our mobile application users' behavior. For more information on the handling of user data on Flurry Analytics, please see their [Privacy Policy](#).
 - Amplitude – an analytics service for mobile apps. For more information on the privacy practices of Amplitude, please see their [Amplitude Terms](#).
 - Visual Studio App Center – owned by Microsoft. Their applicable data protection provisions can be reviewed under the [Microsoft Privacy Statement](#).
- **Business transfers:** If we sell our business or our company assets are acquired by a third party, personal data held by us about our general account users, subscription account users or customers may be one of the transferred assets.
- **Administrative and legal reasons:** If we need to disclose your personal data (i) to comply with a legal obligation and/or judicial or regulatory proceedings, a court order or other legal process, (ii) to enforce our Terms of Use, House Rules or other applicable contract terms that you are subject to, or (iii) to protect us or our contractors against loss or damage. This may include, but is not limited to, exchanging information with the police, courts or law enforcement organizations.
- **Advertising:** We display advertising on the Website and may use remarketing and tracking features. Remarketing features allow us to display advertising in a more targeted manner in order to present advertisements of interest to users, based on their activity on other

websites. Tracking features allow us to collect information about impressions, ad clicks and certain actions that users complete through our Website. This data also helps us evaluate the performance of ad campaigns. Note that we collect pseudonymous data only. We may use the following services for advertising, remarketing, and tracking purposes:

- **Google Ad Manager and Google Ads** – they help us serve and measure the success of ads on our site.

For more information about how Google uses data, please refer to their [Privacy & Terms](#) document as well as [Google's Privacy Policy](#). You can opt out of this by visiting the [Network Advertising Initiative opt-out page](#) or by turning off the personalization of Google ads via their [Ad Settings page](#).

- **Facebook pixel** – allows us to measure, optimize, and build audiences for our advertising campaigns.

You can learn more about Facebook's data policy [here](#). You can manage your personal settings for advertisements on Facebook at [Your Ad Preferences](#). In case you don't have a Facebook account, you can use [Your Online Choices](#) website or [DAA's WebChoices Tool](#) to manage your ad experience.

- **Twitter Conversion Tracking (Twitter Pixel)** – helps us to measure our return on ad expenditure.

For more information about Twitter data processing, please see their [Privacy policy](#). You can adjust the settings in your personal Twitter profile and opt to receive advertising. In case you don't have a Twitter account, you can use [Your Online Choices](#) website or [DAA's WebChoices Tool](#) to manage your ad experience.

- **Google reCAPTCHA** is used to check whether data has been entered by a person or by an automated program. We use this service to protect our services from spam, fraud and abuse. reCAPTCHA analyses the behavior of the visitor using various characteristics and evaluates various information for analysis

purposes (e.g. IP address, visit duration, or the user's mouse clicks). This analysis begins automatically, as soon as the website visitor accesses the website, and runs in the background. Visitors are not informed that an analysis is being performed. The data recorded during analysis is forwarded to Google. More information on Google reCAPTCHA and the [Google Privacy Policy](#) can be found under the following links: [Google's Privacy Policy](#) and [What is reCAPTCHA?](#).

- Note that we do not share any personal information with our advertisers. They can only access general statistics that include the amount of impressions their ads have generated as well as clicks.

Public information on our site

Public Profile

When you create your profile on our Service, other users or visitors can not access your profile.

Security of personal data

We use technical and organizational safeguards to protect your personal data and require third parties with whom we work to do the same.

We use Transport Layer Security (TLS) encryption technology in order to protect certain information that you submit to us. This technology protects you from having your information intercepted by anyone while it is being transmitted to ChefPro or payment processor. While on a secure page, such as our order form, the "lock" icon in the browser window is displayed, confirming that a secure and encrypted connection has been established with the Website. We work hard to ensure that our Service is

secure and that we meet industry standards. We also use other safeguards, such as firewalls, authentication systems (i.e. passwords, and personal identification numbers), and access control mechanisms to control unauthorized access to systems and data. If you have chosen to create an account, you are responsible for doing everything you reasonably can to keep your access details secret. You must not share these details with anyone else.

We also do our best to protect user information offline. All of our users' personal information is restricted to our offices. Only employees who need to see the information to perform their jobs are allowed to access it.

The servers that store personal data are located in a secure environment in a locked facility.

We are constantly improving the ways we secure, store, and process the data we collect, including the addition of physical security measures that help us counter unauthorized access to our systems. However, no method of electronic transmission or storage is 100% secure. Therefore, we cannot guarantee its absolute security.

Children and sensitive personal data

This Website is not directed to wards children who are under the age of 18. We do not knowingly contact or collect personal information from children below the age of 18 years, or sensitive personal data ("racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health

or a natural person's sex life or sexual orientation," etc.). Please consult [Art. 9 GDPR](#) for more information. If you believe we have inadvertently collected such information, please contact us immediately so that we can either obtain special consent or delete the information.

Third Party Sites

Links to other sites

At our discretion we may add links (web links) to other websites from our Website. These websites can be run by third parties with separate and independent privacy policies. We, therefore, have no responsibility nor are we liable for any content, activities or privacy policies of these linked sites. We suggest you read the privacy policy of each and every site that you visit.

EEA and UK users' specific rights

Individuals subject to European and United Kingdom ("UK") data protection laws may have data subject rights in relation to the personal data we hold on them (described in detail below). This may, in and of itself, be subject to limitations and/or restrictions.

If you are located in the EEA or UK, please contact us to exercise your rights.

Accessing data

If prompted, we will confirm whether or not we are processing your personal data and if so, we will provide you with a copy of that personal data along with any other pertinent details. If you require additional copies, we may need to charge a reasonable fee, but this can be discussed and depends on the situation.

Restricting the processing of personal data

You may ask us to restrict or ‘block’ the processing of your personal data in certain circumstances, for example, if you contest the accuracy of the data or object to us processing it. We will notify you before we lift any restriction on processing. If we share your personal data with others, we will notify them of the restriction wherever possible. If prompted, and if it is possible and lawful to do so, we will also notify you with whom we have shared or will share your personal data so you can contact them directly.

Objections

You may:

- ask us to stop processing your personal data at any time, and we will do so. If we are relying on a legitimate interest to process your personal data, then it should not be a problem unless we demonstrate compelling legitimate grounds for processing;
- object to our processing of your data for the purposes of direct marketing at any time. This can be done by clicking the "unsubscribe" button in our marketing emails; and
- refuse to receive service notifications via email (for example, when a user you are subscribed to publishes a chart, idea, etc.). This can be adjusted in the User Settings.

Withdrawal of consent

If we rely on your consent to process your personal data, you have the right to withdraw that consent at any time. This will not affect the lawfulness with which we process your data before receiving notice of your wish to withdraw your consent. We emphasize that we do not generally rely on your consent to allow us to process your personal data if there is another lawful ground available. If we do rely on your consent, we will make this clear to you at that time.

Viewing and correcting data

You have the right to have inaccurate personal data rectified or completed if it is incomplete. In order to do so, each user can view, manage and/or update his/her personal data in the Profile Settings.

If we share your personal data with others, we will notify them of any corrections made whenever possible. If prompted, and where possible and lawful to do so, we will also notify you with whom we have shared your personal data so you can contact them directly if need be.

Deleting data

You have the right to refuse to use our Services and may ask us to delete or remove your personal data in certain circumstances. If we share your data with others, we will notify them of the edits wherever possible. If prompted, and wherever possible and lawful to do so, we will also notify you with whom we have shared your personal data so you can contact them directly if need be.

Please see the "User account deleting" section for more details.

Data retention

We will keep your personal data (1) until you decide to delete your account (upon request), or (2) as required by law or as necessary for legitimate business purposes (i.e. for tax, legal, accounting, fraud, or abuse prevention, and/or other purposes). This data can be stored even after an account is deleted.

Upon expiration of the applicable retention period, we will securely destroy your personal data in accordance with applicable laws and regulations. In some circumstances we may anonymize your personal data so that it can no longer be associated with you. In this case, such data is no longer considered personal.

If you consent to receive marketing communications, we will keep your data until you unsubscribe, which is possible via the 'unsubscribe' button at the end of our marketing emails. Additional methods to unsubscribe may be added in the future.

Lodge a complaint with the data protection authority

If you have concerns about our privacy practices, including the way we handle or have your personal data, you can report it to any competent data protection authority of an European Union member state that is authorized to hear such concerns (you may find European Union Data Protection Authorities' contact information [here](#)) or to the [Information Commissioner's Office \(ICO\)](#), the UK supervisory authority for data protection issues. If you wish to exercise any of these rights, please contact us. Note that we may need to ask you for further information to verify your identity before we can respond to any request.

International data transfers

ChefPro LTDA. is based in the Brazil and Sweden. The information collected through Services will be stored on servers located in the United States, European Union, and other destinations (including outside the EEA), to our service providers and affiliated businesses for the purposes described above. This is necessary to enable you to navigate and use our Services. The data may be transmitted to our service providers and affiliates supporting our business operations (described above).

Note that the countries concerned may not provide the same legal standards for protection of your personal data that you have in the EEA. If we transfer your personal data to countries outside of your country, we will take the necessary steps to ensure your information receives an adequate level of security protection where it is processed and that your rights continue to be protected.

If you would like to receive more information on the safeguards that we implement, please contact us.

California users' specific rights

If you are an eligible California resident, the California Consumer Privacy Act ("CCPA") provides you with specific rights with respect to our collection and use of your personal information. You have the following rights under the CCPA:

- Right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. The list of categories of personal information collected and disclosed about consumers are enlisted in the section 'Personal data that we collect' and the list of categories of third parties to whom the personal information may be disclosed are enlisted in the section 'When would we share personal information'. Please contact us to exercise a data portability request. Separately, we do not sell your personal information.
- Right to request delete personal information we have collected from you. Please see the "User account deleting" section for more details.
- Right not to be discriminated against regarding pricing and services as you exercise any of your rights under the CCPA. We do not offer consumers financial incentives, price differentials, or services in exchange for selling a consumer's personal information.

Contact information

If you have any questions or suggestions regarding personal data processing, please contact us at suporte@chefproapp.com.br.