Pulse 121 Ltd
Privacy Policy

Last updated: October 12, 2023

In this policy, we lay out: what data we collect and why; how your data is handled; and your rights to your data. This policy applies to all products built and maintained by Pulse 121 Limited.

What we collect and why

Our guiding principle is to collect only what we need. Here's what that means in practice:

Identity & access

When you sign up for a Pulse product, we typically ask for identifying information such as your name, email address, and company name. That's just so you can personalise your new account, and we can send you invoices, updates, or other essential information. We sometimes also give you the option to add a profile picture that displays in our products. We'll never sell your personal info to third parties, and we won't use your name or company in marketing statements without your permission either.

Billing information

When you pay for a Pulse product, we ask for your billing details. That's so we can charge you for service, calculate taxes due, and send you invoices. Your credit card is passed directly to our payment processor and doesn't ever go through our servers. We store a record of the payment transaction, including partial (last 4 digits) credit card or bank account numbers, for account history, invoicing, and billing support. We store your billing address to detect fraudulent credit card transactions, and to print on your invoices.

Geolocation data

We log all access to all accounts by full IP address so that we can verify no unauthorised access has happened. We also log full IP addresses used to sign up a product account. We keep this data for 30 days.

Website interactions

When you browse our marketing pages or applications, your browser automatically shares certain information such as which operating system and browser version you are using. This is standard behaviour on all websites, not just ours. We record that information, along with the pages you are visiting, page load timing, and which website referred you for statistical purposes like conversion rates and to test new designs. We sometimes track specific link clicks to help inform some design decisions. These web analytics data are tied to your IP address and user account if applicable and you are signed into our Services. Other web analytics we utilise are described further in the Cookies and Do Not Track section.

Cookies and Do Not Track

We use persistent first-party cookies to store certain preferences, to make it easier for you to use our applications (e.g. remember me functionality), and to support some in-house analytics. We do not use 3rd party cookies.

A cookie is a piece of text stored by your browser. It may help remember login information and site preferences. It might also collect information such as your browser type, operating system, web pages visited, duration of visit, content viewed, and other click-stream data. You can adjust cookie retention settings in your own browser. To learn more about cookies, including how to view which cookies have been set and how to manage and delete them, please visit: www.allaboutcookies.org.

At this time, our sites and applications do not respond to Do Not Track beacons sent by browser plugins because we do not track you across one or more third party services. Our tracking is internal only, and the data we gather is used only to monitor and improve our products and services.

Voluntary correspondence

When you write to Pulse with a question or to ask for help, we keep that correspondence, including the email address, so that we have a history of past correspondences to reference if you reach out in the future.

We also store any information you volunteer like surveys. Sometimes when we do customer interviews, we may ask for your permission to record the conversation for future reference or use. We only do so if you give your express consent.

User contributed content

We offer communication tools for businesses and organisations. You may use our services to communicate with one or more individuals using written messages, images and videos. Any content you share will only be shared with designated recipients . Please note: when you share content with other people, we create a copy of the content in their accounts. If you later delete the content from your account, it will be retained in their account until they delete it or until their account is closed.

Information we do not collect

We do not collect any characteristics of protected classifications including age, race, gender, religion, sexual orientation, gender identity, gender expression, or physical and mental abilities or disabilities. You may provide these data voluntarily, such as if you include a pronoun preference in your email signature when writing into our Support team.

We also do not collect any biometric data. You are given the option to add a picture to your user profile, which could be a real picture of you or a picture of something else that represents you best. We do not extract any information from profile pictures: they are for your use alone.

We do not use any third party tracking, marketing or analytics services

Companies we work with

We use hardware and software provided by external companies to run our business. Your data may pass through or be stored on systems owned or operated by the following companies:

Heroku: https://devcenter.heroku.com/articles/gdpr
Amazon Web Services: https://aws.amazon.com/compliance/gdpr-center/

When we access or share your information
Our default practice is to not access your information. The only times we'll ever access or share your info are:

To provide products or services you've requested. We do use some third-party services to run our applications and only to the extent necessary process some or all of your personal information via these third parties. No Pulse human looks at your data for these purposes unless an error occurs that stops an automated process from working and requires manual intervention to fix. These are rare cases and when they happen, we look for root cause solutions as much as possible to avoid them from reoccurring.

To help you troubleshoot or squash a software bug, with your permission. If at any point we need to access your account to help you with a support case, we will ask for your consent before proceeding.

To investigate, prevent, or take action regarding violation of our Terms Of Use. Accessing a customer's account when investigating potential abuse is a measure of last resort. We have an obligation to protect the privacy and safety of both our customers and the people reporting issues to us. We do our best to balance those responsibilities throughout the process. If we do discover you are using our products for a restricted purpose, we will report the incident to the appropriate authorities.

When required under applicable law. Pulse 121 Limited is a UK company and all data infrastructure are located in the EU. If UK law enforcement authorities have the necessary warrant, criminal subpoena, or court order requiring we share data, we have to comply. Otherwise, we flat-out reject requests from law enforcement when they seek data. And unless we're legally prevented from it, we'll always inform you when such requests are made.

Similarly, if Pulse receives a request to preserve data, we refuse unless compelled by a UK legal authority. In these situations, we notify affected customers as soon as possible unless we are legally prohibited from doing so.

If we get an informal request from any person, organisation, or entity, we do not assist. If you are an account owner who wants to export data from their accounts, please email info@pulse121.com

If we are audited by a tax authority, we may be required to share billing-related information. If that happens, we only share the bare minimum needed such as billing addresses and tax exemption information.

If we sell the company. Finally, if Pulse 121 Limited is acquired by or merged with another company — we don't plan on that, but if it happens — we'll notify at least 30 days before any data about you is transferred and becomes subject to a different privacy policy.

Your rights with respect to your information

At Pulse, we apply the same data rights to all customers, regardless of their location. These rights include:

Right to Know. You have the right to know what personal information is collected, used, shared or sold. We outline both the categories and specific bits of data we collect, as well as how they are used, in this privacy policy.

Right of Access. This includes your right to access the personal information we gather about you, and your right to obtain information about the sharing, storage, security and processing of that information.

Right to Correction. You have the right to request correction of your personal information.

Right to Erasure / “To be Forgotten”. This is your right to request, subject to certain limitations under applicable law, that your personal information be erased from our possession and, by extension, all of our service providers. Fulfilment of some data deletion requests may prevent you from using Pulse services because our applications may then no longer work. In such cases, a data deletion request may result in closing your account, but we will let you know if that is the case.

Right to Complain. You have the right to make a complaint regarding our handling of your personal information with the ICO.

Right to Portability. You have the right to receive the personal information we have about you and the right to transmit it to another party.

If you have questions about exercising these rights or need assistance, please email us at info@pulse121.com. For requests to delete personal information or know what personal information has been collected, we will first verify your identity using a combination of at least two pieces of information already collected including your user email address. If an authorised agent is corresponding on your behalf, we will first need written consent with a signature from the account holder before proceeding.

How we secure your data

All data is encrypted via SSL/TLS when transmitted from our servers to your browser. Our database backups are also encrypted.

What happens when you delete data in your product accounts

In many of our applications, we give you the option to delete data. Anything you delete becomes immediately inaccessible in your account. We also have some backups of our application databases, which are kept for up to 30 days. These backups are used for recovery of data in the event that our systems fail and our entire database needs to be restored. Backups are not used to restore data for a single account or subset of accounts because it is time and cost prohibitive.

Contact

If you have a question about any of the Terms of Service, please email info@pulse121.com