



Privacy Policy

Trialflare

Trialflare (the “service”, etc.) is provided by Seastorm Limited.

Seastorm Limited ("Seastorm", "we", "us", etc.) considers your privacy to be very important. We will therefore process and use your data in a secure manner in accordance with the General Data Protection Regulations (GDPR) and other applicable laws and regulation. In this document we set out how and why we use your information.

Seastorm is a limited company registered in England and Wales, with company number 11867862. Our address is 141 Albany Road, Cardiff, CF24 3NT. You can contact us on hello@seastorm.co with any questions or concerns.

Scope of this Policy

This policy applies to all users and participants of the Trialflare service. This includes usage of our web and mobile apps, and any other approved clients.

This policy also applies to visitors to our website (<https://trialflare.com> or its subdomains), even if the visitor is not a Trialflare user or participant.

This policy does not apply if you contact us (e.g. via email or otherwise), engage with us in any project or consultancy agreement, engage with us for billing or payment, for any marketing or sales activity, or for anything else not directly related to Trialflare. In these cases, our general Seastorm Limited privacy policy applies, which can be found at <https://www.seastorm.co/privacy>.

This policy also does not apply if you follow links to any resources outside of our control or services.

For the purposes of relevant data protection regulation, we act as data *processor* for all users, data and participants on behalf of the host organisation (i.e. the licence-holding organisation or the organisation running a trial), who is the data *controller*.

Cookies

Our website does not use cookies to track visitors to the site. However, cookies are used by our live chat technology in order to remember your chat for the next time you visit.

What Data do we Collect?

In this section we identify the key points at which we collect data, and the purpose for the collection.

When you visit our website(s)

When you visit our website(s) or web application(s) using a web browser, we collect some data about your computer and the way our services are used by you, even if you don't have an account. We do not collect your name or other personal details about you at this stage, but we may process information such as your computing device's country and details about your browser and where you arrived from. We do this for observing aggregated usage of our services, so that we can better understand how to improve our services for their audiences. The legal basis for processing this data is a legitimate interest in recording aggregated analytics data for improvement purposes and to see how often people visit our website.

When you join us as a user

The service allows you to register for an account. This is the primary way by which we collect personal data from you, since such data is needed in order to identify you when you want to login and use these services. We may also use your email address to update you on platform updates and notifications, which you can control. When signing-up we collect your email address, name, and password.

We ask you for consent to this policy when you create or enrol an account, and the legal basis for processing this data is a legitimate interest in being able to provide services to you and to also to enable us to deliver contracted services as a supplier to your (or the host) organisation.

When you use our services as a user

We do not ask for or collect any additional personal data (further to the clauses above) as you use our services as a logged-in user. We do collect data relating to trials, configurations, and settings, and other information you wish to provide.

You can modify your account details (including personal data) using your account settings.

When you join us as a participant

The service allows you to login to a trial as a participant, however we do not ask for or collect personal data relating to participants as part of usual operation. When you login to a trial, we collect a participant ID and trial code for the purposes of granting you access to the trial, however your participant ID should not contain any personally-identifiable information.

As a participant, the data you provide is protected by the privacy policy or the terms of the host organisation (i.e. the organisation running the trial), and you will have the opportunity to read these terms before you agree to join the trial. The host organisation may maintain "deblinding" information, which enables them to determine who a particular participant is from their ID. It is that organisation's responsibility to ensure that this deblinding information and process is kept safe and secure.

If you are a participant and make use of the additional "eConsent" feature when joining a trial, you have the option of providing an email address and/or a phone number. We collect this data in order to complete the eConsent verification process. This personal information is collected and processed securely by us on behalf of the host organisation.

When you use our services as a participant

During a trial, you will be asked to provide information in relation to the trial. We collect this data for the purposes of running the trial. This data is protected by the privacy policy or terms of the host organisation, to which you would have agreed during the login process.

Subprocessors

We work with selected subprocessors to help run our services, as described below.

Amazon Web Services (AWS): We use AWS to host and run our services.

Mailgun: We use Mailgun for the purposes of sending emails to registered users (for example, password reset emails or notifications, or during the eConsent verification process). To send the mail, we provide this subprocessor with your email address.

Twilio: We use Twilio for the purposes of sending SMS (text messages) (for example, during the eConsent verification process). To send the SMS, we provide this subprocessor with your phone number.

Who can Access your Data?

Seastorm staff responsible for managing or maintaining your organisational account can view your account and its data, with the exception of passwords, which are fully encrypted.

Other users in your team may be able to view your profile information (such as your name or email) if they have the appropriate permissions (e.g. they are administrators).

As a participant, the data you provide as part of eConsenting, accessing or participating in a trial can be viewed by relevant staff in your trials' host organisation(s).

We may be required to provide data to legal authorities if we receive such a request or warrant. If Seastorm is purchased or otherwise has its control transferred to another organisation or body, then data we hold will also be transferred to the new business controller. However your data will still only be used for the same purpose for which it was originally supplied to us. In any case, we act and will take steps with the aim of ensuring your privacy is protected.

How Long do we Keep Data for?

We keep your account data (e.g. name and email address) for as long as your account is active. You can fully and irreversibly delete your account at any time from within your account settings.

Content created by you or your organisation (e.g. trials and data types) will be kept until they are deleted by someone with the correct permissions (e.g. the person who created it, or an administrator).

As a participant, retention of your data is controlled by your trials' host organisation(s). You should reach out to a trial administrator or the Trialflare team for more information on this.

When a licence ends (and is not due to be renewed), we work with the organisation to off board data in-line with a pre-agreed plan.

Please note that data held in backup systems may be held for up to an additional 30 days after it is deleted from our services.

Where is your Data Stored and Processed?

We store and process all data within our UK data centres, and this includes backups. We use Mailgun's EU servers for transmitting email.

How do we Protect your Data?

Your data is well-protected. We use industry grade practices to help prevent against unauthorised access. This includes fully encrypting data in-transit (e.g. between your device and our servers,

and between our servers) and at-rest (e.g. when it is saved onto the hard disks of our database servers).

We use data centres that practice advanced protection mechanisms to prevent unauthorised access.

Child Safety

Children under the age of 16 are not allowed to use our services or to directly provide us with personal data. As such, we do not knowingly store or process personal data relating to children under the age of 16.

Your rights

As an individual, you have rights with regard to personal data processed by us. Should you wish to exercise any of these rights then please get in touch with the email address shown on this policy. We will endeavour to action any rights within one business week.

Right to access

At any time you have the right to know about any personal data we hold about you.

Right to correct

You have the right to have your personal data corrected or updated or deleted.

Right to object

You have the right to object to us processing your data.

Right to data transfer

You have the right to request your data in a sensible format such that it can be transferred to a different provider or system.

Rights relating to automated processing

If you feel you are being affected by us carrying out actions as a result of an automated process, to which you object to, you can object. We do not use automated decision making in a way that will affect an individual.

Withdrawal of consent

If you have provided consent for us to process your personal data, you can withdraw this consent at any time. This can be achieved by deleting your account, or by reaching out to us.

Complaints

If you would like to complain about the way in which we have handled your personal data, or about this policy, then please get in touch with us using the details in this policy.

You may also get in touch with the Information Commissioner's Office (<https://ico.org.uk>) to raise a complaint.