



Privacy Policy

V.3.2.

ISMS-POL-002

JULY 2026

ISSUED BY:

Spatial Networks, Inc

Table of Contents

Table of Contents..... 1

Revision History..... 2

Overview..... 3

Purpose and Effect..... 3

Your Personal Information..... 3

How We Use Your Personal Information..... 5

Data Security, Storage, and Retention..... 6

Data Rights..... 7

Disclosing Your Personal Information..... 9

External Links..... 11

International Data Transfers..... 11

Data Privacy Framework..... 12

Mobile App Permissions (iOS)..... 13

Children..... 14

Changes to this policy..... 15

Contact..... 15

Revision History

Version	Date	Change Made	Author
1.0	06/2023	Issued first Fulcrum-internal social version	Rob Smithers
2.0	03/15/2025	Annual review and update	José Vargas, Rob Smithers, Ángela Arango
2.0	03/15/2025	Review and update	Trey Hyde, Jake Freivald, Greg Hunt
2.0	07/01/2025	Approval	Jake Freivald, Greg Hunt
3.0	02/03/2026	Add Data Privacy Framework	Jose Vargas
3.1	05/04/2026	Data Privacy Framework modification	Angela Arango
3.2	07/10/2026	Add Mobile App Permissions (iOS)	Angela Arango

Overview

This privacy policy (“Policy”) applies to Spatial Networks, Inc. (“Spatial Networks”, “we,” “us,” or “our”), which proudly develops the Fulcrum platform, and the information that we collect from or about our users (“you,” or “your,”) through our platform, website (<https://www.fulcrumapp.com/>), applications, services, and/or software (hosted at <https://web.fulcrumapp.com> and <https://api.fulcrumapp.com>, collectively, the “Service”).

By indicating your acceptance of this Policy, you hereby accept the terms contained herein.

Purpose and Effect

Your use of the Service is voluntary. We must obtain personal information about you in order to provide you with certain features of the Service. By using the Service or requesting that we provide the Service to you, you agree to disclose certain of your personal information to us and authorize us to use and disclose your personal information pursuant to the provisions of this Policy.

Your Personal Information

We collect personal and other information from you directly when you provide it to us through the Service. We also collect personal and other information that our customers process through our Service. We further automatically collect certain information about you and your computer, smartphone, or other device when you use, access, or interact with the Service. We may also collect information from third parties in relation to providing you the Service.

Spatial Networks acts as a data processor or a service provider to its customers (who are, in turn, data controllers) for the majority of the personal information that it processes through the Service. Accordingly, for personal information that it processes in this processor or service provider capacity, Spatial Networks complies with relevant legal requirements imposed on data processors or service providers.

If you are a customer, before your use of the Service, we may request certain personal information about yourself, including, but not limited to, your: (i) first name and last name; (ii) email address; (iii) mailing address; (iv) telephone number(s); (v) organization information; and (vi) credit card information. Such information is considered “personal information,” which means information that can directly or indirectly identify you as a natural person. There are two types of personal information we may collect, including “regular data” and “special categories of personal data.” Regular data may include your name, address, email address, photo, IP address, geographical location data, online behavior (cookies), and profiling and analytics data. Special categories of personal data would include race, religion, political opinions, trade union membership, sexual orientation, health information, biometric data, and genetic data. Not all such personal data is collected by us.

Additional information, which may not identify you (as described below) and other personal information may include: browser type and version, operating system, information about your visits to and use of the Service including the referral source, length of visit, page views, and website navigation paths; email address, profile information that you voluntarily provide to us, including, for example, profile pictures, gender, birthday, relationship status, interests and hobbies, educational details, employment details, and credit card information. Information may also include your click history, the times and dates at which you access the Service, the particular portions of the Service you use, and the details of transactions you conduct using the Service.

We use cookies in the Service. For more information about our use of cookies, please see our [Cookie Policy](#). In addition, the Service or the emails that you receive from us may use an application known as a “web beacon” (also known as a “clear gif” or “web bug”). A web beacon is an electronic file that usually consists of a single-pixel image. It can be

embedded in a web page or in an email to transmit information, which could include personal information. For example, it can allow an email sender to determine whether a user has opened a particular email.

We may partner with certain third parties to collect, analyze, and use the personal and other information described in this section. For example, we may allow third parties to set cookies or use web beacons on the Service or in email communications from us. This information may be used for a variety of purposes, including online interest-based advertising.

How We Use Your Personal Information

We use the information that we collect for a variety of purposes. Our legal bases for processing your personal information are: 1) our legitimate interest in running and maintaining our business; 2) performance and fulfillment of our contracts; 3) your consent; and 4) compliance with our legal obligations. In many instances, more than one of these legal bases apply to the processing of your personal information.

Personal information submitted to us through the Service will be used for the purposes specified in this Policy. We may use your personal information for the following:

- Administering our website, application, and business;
- Personalizing our website tools and/or databases for you;
- Enabling your use of the Service;
- Sending you software or software tools purchased through our app or website;
- Supplying the Service to you;
- Sending statements, invoices, and payment reminders to you, and collecting payments from you;
- Sending you marketing and non-marketing communications;
- Sending you email notifications that you have specifically requested;
- Providing third parties with statistical information about our users (but those third parties will not be able to identify any individual user from that information);

- Providing information to our processors or sub-processors, where appropriate;
- Dealing with inquiries and complaints made by or about you relating to the Service;
- Keeping our app and website secure and preventing fraud;
- Serving you advertisements;
- Verifying compliance with the terms and conditions governing the use of the Service; and other uses, which may be added hereto.

We may link information gathered through the Service with information that we collect in other contexts. But in that event, we will handle the combined information in a manner consistent with this Policy.

If you submit personal information for publication on our website, we will publish and otherwise use that information in accordance with the license you grant to us.

Data Security, Storage, and Retention

Personal information will be stored in the cloud by our processors or sub-processors. Personal information will be stored in a manner that ensures appropriate security, integrity, and confidentiality and secured against unauthorized processing, accidental loss, destruction, or damage. We will take reasonable technical and organizational precautions to prevent the loss, misuse, or alteration of your personal information. We will store the personal information you provide on our secure servers. However, the transmission of information over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet. You are responsible for keeping the password you use for accessing our app or website confidential.

We retain personal information as long as necessary to fulfill the purpose for which that information was collected or as required or permitted by law. We do not retain personal information longer than is necessary for us to achieve the purposes for which we collected it.

Data Rights

Depending on your jurisdiction, you may have certain rights concerning your personal information.

For example, you may have the right to request that your personal information be provided to you in a portable manner. Portability means the personal information will be stored in a manner that allows you to obtain and reuse your personal information for your own purpose by transferring it to a different environment. Upon your written request, you will be provided with the ability to access your personal information to verify its accuracy, download it in an easily portable format, or request a copy of your personal information being processed.

You further have the right to object in writing to the processing of your personal information. In such a case, the personal information will not be processed, unless we demonstrate compelling and legitimate grounds for the processing that override your interests, rights, and freedoms, or we require the data to establish, exercise, or defend legal rights. You further have the right to object to the processing of your personal information for the purpose of direct marketing, including profiling. Where personal information is processed for scientific and historical research purposes or statistical purposes, you have the right to object, unless the processing is necessary for the performance of a task carried out for reasons of public interest. If you object to the processing of your personal information, you agree to the termination of your access to the Service in the event that we determine, in our sole discretion, that we are unable to provide the Service due to your objection to the processing of your personal information. This objection right is given free of charge, although we may charge a reasonable fee for repetitive, manifestly unfounded, or excessive requests.

Upon termination of the Service for any reason, and upon your written request, your personal information may be erased. When we erase personal information, we do so in a way that prevents that information from being restored or reconstructed. Additionally,

you have the right at any time to demand that inaccurate or incomplete personal information be erased or rectified.

You also have the right to obtain the following information:

- Confirmation of whether, and where, we are processing your personal information;
- Information about the purposes of the processing;
- Information about the categories of data being processed;
- Information about the categories of recipients with whom the data may be shared;
- Information about the period for which the data will be stored (or the criteria used to determine that period);
- Where the personal information was not collected from you, information as to the source of the personal information, and information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on you.
- You may restrict processing of your personal information, meaning the personal information may only be held by us, and may only be used for limited purposes, if the accuracy of the personal information is contested (and only for as long as it takes to verify accuracy); the processing is unlawful and you request restriction (as opposed to exercising the right to erasure); we no longer need the personal information for its original purpose but the personal information is still required by us to establish, exercise, or defend legal rights; or verification of overriding grounds is pending in the context of an erasure request.

You may opt out of receiving marketing emails from us by following the instructions in those emails or by emailing us at privacy@fulcrumapp.com.

In addition to the above rights, you may have additional rights under the laws of various US and international jurisdictions. These rights may include:

- The right to opt out of the sale or sharing of your information;
- The right to opt out of targeted advertising;
- The right to limit our use of certain automated decision-making processes.

To exercise any of the rights listed above, please contact us via email at privacy@fulcrumapp.com. Upon your request for any of the above-referenced information, we will, within one month of receiving your written request, provide such requested information. In the event we fail to meet this deadline, you may complain to the governing Data Protection Authority and may seek a judicial remedy, depending on the jurisdiction. In the event we receive a large number of requests, or complex requests, the time limit may be extended by a maximum of two additional months.

We will not refuse to give effect to your rights unless we cannot identify you through the use of reasonable efforts to verify your identity. Where we have reasonable doubts as to your identity, we may request the provision of additional information to confirm your identity.

Additionally, you may authorize an agent to make a request on your behalf. To designate an agent, please provide a written and signed document by both you and the agent that authorizes the agent to act on your behalf. You may also use a power of attorney. We will still require you to provide information to allow us to reasonably verify that you are the person about whom we collected personal information.

If you are a resident of California, please review our [California Privacy Notice](#) for additional rights that may apply to you.

Disclosing Your Personal Information

We may disclose your personal information to any of our employees, officers, insurers, professional advisers, agents, suppliers or subcontractors, service providers, subsidiaries, or parent companies as reasonably necessary for the purposes set out in this Policy. In addition, we may disclose your personal information:

- To the extent that we are required to do so by law;
- In connection with any ongoing or prospective legal proceedings;

- To establish, exercise, or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);to the
- To the Purchaser (or prospective purchaser) of any business or asset that we are (or are contemplating) selling; and
- To any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.
- We may also disclose your personal information for analytics and interest-based advertising purposes:

Analytics. We partner with certain third parties to obtain the automatically collected information discussed above and to engage in analysis, auditing, research, and reporting. These third parties may use web logs or web beacons, and they may set and access cookies on your computer or other device. You may opt out of the use of cookies . **For more information please review our [Cookie Policy](#).**

Interest-based advertising. The Service also enables third-party tracking mechanisms to collect information about you and your computing devices for use in online interest-based advertising. For example, third parties may use the fact that you visited our Service to target online ads to you. In addition, our third-party advertising networks might use information about your use of our Service to help target advertisements based on your online activity in general. For information about interest-based advertising practices, including privacy and confidentiality, visit the [Network Advertising Initiative](#) website or the [Digital Advertising Alliance](#) website.

The use of online tracking mechanisms by third parties is subject to those third parties' privacy policies, and not this Policy. If you prefer to prevent third parties from setting and accessing cookies on your computer or other device, you may set your browser to block cookies. Additionally, you may remove yourself from the targeted advertising of companies within the Network Advertising Initiative by opting out [here](#), or of companies participating in the Digital Advertising Alliance by opting out [here](#). Our Service does not currently respond to "do not track" signals.

External Links

The Service may contain links to third-party websites. If you use these links, you will leave the Service. We have not reviewed these third-party sites and do not control and are not responsible for any of these sites, their contents, or their privacy policies. Thus, we do not endorse or make any representations about them, or any information, software, or other products or materials found there, or any results that may be obtained from using them. If you decide to access any of the third-party sites listed on our website, you do so at your own risk.

International Data Transfers

The information that we collect through or in connection with the Service is transferred to and processed in the United States for the purposes described above. Spatial Networks may subcontract the processing of your data to, or otherwise share your data with, affiliates or third parties in the United States or countries other than your country of residence. Although the data protection laws in these countries may be different from, and less stringent than, those in your country of residence, Spatial Networks Inc. follows a Vendor Management Policy to gain reasonable assurance that third-party subprocessors are in compliance with Spatial Networks' Information Security policies. By using the Service or by providing any personal or other information to us, you expressly consent to such transfer and/or processing. You can request these policies and other Information Security information through our [Trust Center](#).

Data Privacy Framework

Spatial Networks, Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. Spatial Networks, Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit <https://www.dataprivacyframework.gov>.

In compliance with the EU-U.S. DPF Principles, Spatial Networks, Inc. commits to resolve complaints about our collection or use of personal information. EU and UK individuals with inquiries or complaints regarding our DPF policy should first contact Spatial Networks, Inc. at: privacy@fulcrumapp.com.

Spatial Networks, Inc. has further committed to refer unresolved DPF complaints to JAMS, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact or visit <https://www.jamsadr.com/dpf-dispute-resolution> for more information or to file a complaint. The services of JAMS are provided at no cost.

Individuals have the right to access their personal data, which may be stored on Spatial Networks, Inc. systems.

Except for the entities outlined in this Policy, Spatial Networks, Inc. does not disclose any personal data provided by our users to any other users or entities. Some personal data is required to operate a Fulcrum account. Users may cancel their account to remove this

data. Any personal data collected by users will be removed by Spatial Networks, Inc. upon written request of the user or the data subject.

Spatial Networks, Inc. is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Under certain conditions, a user or data subject may invoke binding arbitration regarding personal data stored by Spatial Networks, Inc.

Spatial Networks, Inc. is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Spatial Networks, Inc. remains liable under the DPF Principles if an agent processes personal information covered by this Policy in a manner inconsistent with the Principles, except where Spatial Networks, Inc. is not responsible for the event giving rise to the damage

Mobile App Permissions (iOS)

The Fulcrum iOS application requests the following device permissions. Each permission is optional where technically possible and is only activated when you use the relevant feature. No data collected through these permissions is sold to third parties.

Permission	What is accessed	Why it is needed
Location	Device GPS coordinates (while the app is in use).	To attach location data to collected records and to display records on a map.

Camera	Camera hardware and live preview.	To capture photos and video as part of data collection, and to scan barcodes. No images are taken without your action.
Microphone	Device microphone input.	To record audio fields within a data collection form. Audio is only recorded when you explicitly start a recording.
Photo Library (read)	Photos and videos stored on the device.	To allow you to attach existing photos from your library to records.
Photo Library (write)	Ability to save to the photo library.	To save captured photos to your device library when you choose to do so.
Bluetooth	Nearby Bluetooth devices.	To connect to external GPS receivers for high-accuracy location data collection.
Face ID / Biometrics	Face ID authentication result.	To authenticate your identity when unlocking the app. Biometric data never leaves your device — authentication is handled entirely by iOS.
Speech Recognition	Microphone audio processed by Apple's on-device/cloud speech engine.	To power the FastFill voice input feature. Audio is processed by Apple's Speech framework in accordance with Apple's privacy policy.

Children

Content on the Service is directed at individuals over the age of 18 and is not directed at children under the age of 13. We do not knowingly collect personally identifiable information (PII) from children under the age of 13.

Changes to this policy

We may make changes to the Service in the future and as a consequence will need to revise this Policy to reflect those changes. We will post all such changes on the Service, so you should review this page periodically. If we make a material change to the Policy, you will be provided with appropriate notice.

Contact

If you have any questions about our privacy policy, please contact us at privacy@fulcrumapp.com.