Findmyshift - Privacy policy

Last updated: 25/01/2021

The data we collect

Input data

As a data-driven application for scheduling staff, we offer our users the ability to enter a wide range of staff data, though none of this is mandatory. The data collected includes staff names, email addresses, phone numbers, job titles, departments, dates of birth, payroll IDs, shifts times, salaries, pay rates, day rates, time off, time off allowances, and timesheets.

As employees log in and use the service, they too have the option to provide data - such as timesheets, clock in/out times, shift requests, cancellations, time off requests, notice board messages, notification preferences, and profile pictures.

Metadata

Aside from the data that users knowingly provide, we also record metadata, such as IP addresses, URLs, timestamps, and information about the user's browser. This data is typically used for auditing and security purposes. Sensitive metadata (such as an employee's latitude/longitude, or photographs of employees as they clock in/out) is only recorded if the employee consents.

Cookies

Findmyshift also uses a number of cookies to function, however all users can view which cookies we use and adjust their privacy settings at any time to opt-out of some non-essential cookies. Certain other cookies are required for Findmyshift to run. For a more detailed explanation about the cookies that are used on Findmyshift please visit our cookie policy.

Reasons for collecting data

For Findmyshift to be of value as a scheduling tool, it is necessary for data to be collected and stored. Without data, Findmyshift would not be able to maintain a staff list for a manager, forecast labour costs, display rosters, or send notifications to staff about when they are working next.

Findmyshift only ever uses your data within its software platform for the purposes of scheduling, reporting and communication. None of the data we collect about you is ever shared, sold, profiled, or used for any sort of marketing.

GDPR compliance

The lawful grounds for collecting data

The GDPR requires that all processing activities are based on a specific lawful ground. There are six in total, but we only rely on the following lawful grounds:

1. the data we collect is necessary for the correct performance of the contract between Findmyshift and its users, such as the delivery of services via the Findmyshift platform, invoicing the user, and being able to respond to requests from users;
2. in some cases, we are under a legal or regulatory requirement to process certain types of data, for example for tax purposes;
3. in other cases, we have requested your explicit consent to collect and process certain types of data.

How long do we store your data?

We only keep your data for as long as it is necessary for the purposes indicated above. After this, we undertake to delete your data within a reasonable time limit.

Safeguarding the data we collect

Safeguarding customer data is one of Findmyshift's highest priorities, and we go to extensive lengths to ensure data is kept private in transit, in our systems, and in our backups.

To keep your data private in transit, we enforce mandatory SSL connections, making it impossible for any third party to view the data you are transmitting.

To prevent personal data from being stolen, it is always encrypted (automatically and in real-time) before it is stored. And similarly, all passwords are salted and hashed before they are stored, so the actual password can never be read.

Moreover, Findmyshift's servers reside in secure, world-class data centres, protected by an array of intrusion detection systems. Findmyshift engineers are made aware of any suspicious activity in real-time. In the unlikely event of a data breach, Findmyshift is committed to notifying any affected individuals within 48 hours.

The following table shows the various privacy and security measures taken during different stages of the data lifecycle within Findmyshift.

Privacy during transit:	Findmyshift ensures that all interactions between end-users and our services are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols.
Privacy during storage:	Findmyshift ensures that all personal data is encrypted when stored within its service.
Backups:	Findmyshift ensures that all data backups are also encrypted before being replicated for redundancy.
Two-factor access controls:	Findmyshift offers end-users the option to enable two-factor authentication on their account.
Secured network:	Findmyshift provides a high level of network security with intrusion detection, active server monitoring, rate limiting, firewalls, dynamic IP blacklists, mandatory SSL and more.

Data relating to children

Data controllers may not use Findmyshift to process the personal data any individual under the age of 16. If data controllers have staff that are under the age of 16, they must anonymise the data before entering it in to Findmyshift.

Sensitive data

Data controllers may not use Findmyshift to process sensitive data. Sensitive data includes a person's racial origin, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data about their health, data about their sex life or sexual orientation, criminal convictions, and criminal offences and their related security measures.

Non-EU/EEA transfers

Findmyshift's normal (regular) data processing activities all occur within the EU/EEA, with all databases, servers and backups located in EU/EEA data centres.

On occasion (and only when necessary) data may be transferred to a third country if:

1. the third country has been deemed by the EU Commission to ensure an appropriate level of protection, or;
2. the recipient of the data guarantees an acceptable level of data protection in accordance with EU standard contractual clauses for the transmission of personal data, or;
3. there are other safeguards in place that permit such a transfer.

Sharing data with third-parties

We do not share any data with third-parties unless the third-party is involved in the delivery of the service, is GDPR compliant and we have a sub-processor agreement in place, or we are required to share the data by law. The third-party sub-processors we currently work with are:

Service	Providers
Hosting and data storage	Google, Inc. Amazon Web Services, Inc.
Customer support	Slack Technologies, Inc. FrontApp.com, Inc.
SMS messages and push notifications	Google, Inc. Twilio, Inc. Clickatell Ltd.
Payment processing	Stripe, Inc.
Visitor and site usage analytics	Google, Inc. Hotjar Ltd.

Your rights

Accessing your data

To find out if Findmyshift is processing your data and/or to obtain a copy of the personal data we process, you can submit a "right of access" request using this form.

Correcting your data

Staff members can log in to add, edit or remove their first names, last names, phone numbers, email addresses, dates of birth, and contact preferences. Any other change to personal data must be made by their employer (the data controller).

Employers (data controllers) can log in to add, edit, or remove any of their own data and that of their employees.

Deleting your data

The exact method of deletion depends on whether you are an owner of a team or a staff member.

Owners of teams who would like to delete a team, its staff members, and all associated data are able to use the "Delete" button at the bottom of the team's "Settings" page. Once there are no more rosters/teams in an owner's account, a "Delete my account" option will appear on your "Account" page.

Staff members who would like their personal data deleted from Findmyshift should contact their employer (the data controller) and request for their profile to be anonymised. Administrators can anonymise a staff member's profile by clicking the "Delete" button at the bottom and selecting the "Anonymise" option.

Anonymising a staff member's profile will replace their first name and last name with initials, remove their date of birth, profile picture, email address, and their mobile and alternate phone numbers. Anonymising a staff member's profile will not remove data entered in any custom columns, so it's important to manually check and remove any personal data.

Downloading your data

All users (administrators, managers, employees) will find a "Download my data" option under their account. This option will allow them to compile and download all the data that is associated with their account in several different machine-readable and human-readable formats.

Objecting to the processing of your data

If Findmyshift is processing your data on behalf of a data controller and you would like to object, you can request that we stop using this form. Once you submit your request we will send you an email to verify your email address.

If you are a data controller and would like your data removed in its entirety, you can use the "Delete" button at the bottom of the team's "Settings" page. Once there are no more rosters/teams in an owner's account a "Delete my account" option will appear on your "Account" page.

Find out more

If you'd like to find out more about any of the questions above or have a specific question about how we protect your data, then please don't hesitate to get in touch through email and live chat. You can also email us directly at help@findmyshift.com.