Findmyshift - GDPR compliance statement

Last updated: 19/05/2019

About the GDPR

The GDPR was introduced by the European Union to protect the privacy of EU residents. At its core, the new legislation gives individuals a greater say over what, how, why, where, and when their personal data is used, processed, or deleted.

The GDPR also requires organisations to implement stricter security protocols, record any data processing activities under their responsibility, and ensure any data breaches are reported to the data subjects without delay after being made aware, within a maximum time frame of 72 hours.

The GDPR requires compliance from any organisation with 250 staff members (or more) that stores or processes the personal data of EU residents, regardless of the organisation's location. If an organisation does not work with the personal data of EU residents but acts as a data processor the GDPR may still apply, as without the compliance of the data processor, their customers could be deemed non-compliant.

Smaller organisations with fewer than 250 staff members may be exempt if they do not risk the rights and freedoms of individuals, only process data occasionally, are not processing data relating to criminal convictions/offences, and are not processing sensitive data, such as an individual's race, ethnic origin, religion, etc.

Findmyshift's compliance

Findmyshift is compliant with all aspects of the GDPR, which covers the privacy of data subjects, the security of their data, and their control of their data.

Organisations that use Findmyshift must accept our Data Processing Agreement to remain GDPR compliant, and (if applicable) provide details of their Data Protection Officers (DPOs) and EU/EEA representative via the "Settings" > "Data protection" page of their teams.

Security and privacy of customer data

Findmyshift treats the security and privacy of customer data as its highest priority. Some of the policies we enforce include mandatory SSL connections (both internally and externally), real-time encryption/decryption of all personal data in our database, irreversible password salting and hashing, and further encryption for all offsite/cold storage backups.

Transferring personal data outside the EU or the EEA

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 permissible - that is if the third country has been deemed by the EU Commission to ensure an appropriate level of protection, 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 there are other safeguards in place that permit such a transfer.

Right of erasure and rectification

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, they will see a "Delete my account" under their "Account" page.

Employees who would like to update or remove their personal data from Findmyshift should contact their employer (the data controller).

To ensure historical reports remain accurate, Findmyshift gives administrators the ability to anonymise a staff member's profile (instead of deleting it), 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 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.

Data portability

All users (administrators, managers, employees) can use this form to compile and download all the data that is associated with their email

address. The downloaded data is provided in JSON format and is machine readable.

Subject access requests

If an individual would like to enquire as to whether Findmyshift is (or was) processing their personal data then they can request a report of the processing activities using this form.

Data processing objections

If an individual would like to restrict or object to the processing of their personal data, they can make a request using this form. Once the individual's email address is verified our team will ensure their data is anonymised.

If an individual would like to remove previous objections to the processing of their personal data, they can make a request using this form. Once the individual's email address is verified the processing will be permitted.

Responding to data breaches

In the unlikely event that personal data is stolen, Findmyshift will notify all data controllers and data subjects that are affected within 48 hours by email.

Data retention

Findmyshift does not remove personal data uploaded by data controllers until it is deleted by the data controller, or the data controller makes a request to Findmyshift for it to be deleted. After personal data is deleted from our production servers, it may still reside in our offline backups for up to 24 months, however if a backup is restored all efforts will be made to ensure the data is deleted again.