

# Data and Privacy Policy

## MAF Wingmate

Version 1.0, Dated 7 February 2024

We want you to know exactly how we collect and use your data before you start using the "MAF Wingmate app". Please take a few moments to read the following detailed information about the "MAF Wingmate app", before acknowledgment and use of the app.

On this page, we provide you with information regarding the processing of your data on the **MAF Wingmate app** (referred to below as the 'app'). For further information about how **Mission Aviation Fellowship UK** handles personal information please click here: <https://www.maf-uk.org/privacy/>.

How we collect and use your data will depend on how you interact with us, the app and the specific services you use. We only collect, use or share your data where we have a legal basis for doing so. The following describes how and why we might collect, store, use, and/or share ('process') your information when you use our services ('services'), such as when you:

- Download and use our mobile application
- Engage with us in other related ways, including events, sales and marketing

## Summary of key points

*This overview summarises the main points from our privacy policy. To learn more about any of these topics, or if you want to learn more about what we do with any information we collect, please review the privacy notice in full.*

**Who provides the service and who is processing my data?** The organisation in charge of your data, following the rules of the UK General Data Protection Regulation (UK GDPR, is Mission Aviation Fellowship UK, Charity Number 1064598 in England and Wales. The app and technical infrastructure are operated by If Give Limited (Company Number 13889210).

**What personal information do we process?** When you visit, use, or navigate our services, we process personal information depending on how you interact with us and the services, the choices you make, and the products and features you use.

**Do you process any sensitive personal information?** We do not process sensitive personal information. We do not knowingly process the personal information of vulnerable individuals or children under the age of 18.

**Do you receive any information from third parties?** We do not receive any information from third parties.

**How do you process my information?** We process your information to provide, improve, and administer our services, to communicate with you, for security and fraud prevention, and to comply with regulations and the law. With your consent, we or third-parties may also use your data for creating new services, conducting academic research, or other approved purposes. We process your information only when we have a valid legal reason, for example, your explicit consent, to do so.

**In what situations and with which parties do we share personal information?** We may share information in specific situations and with specific third parties, for example, if you gave your consent to do so, or to comply with fundraising regulations, e.g. to process Gift Aid donations, or to facilitate payment processing.

**How do we keep your information safe?** Our data processor and all sub-processors have organisational and technical processes and certified procedures in place to protect your personal information. However, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure.

**What are your rights?** Under UK privacy laws, you have specific rights concerning your personal information based on your geographical location. This policy aims to help you understand your privacy rights under the applicable UK privacy regulations.

**How do you exercise your rights?** The easiest way to exercise your rights is by using our data processing and communication settings in the app (in the section "more"), or by contacting us. We will consider and act upon any request following the applicable data protection laws.

# Table of Contents

<b>Summary of key points</b>	<b>1</b>
<b>1. Data Controller</b>	<b>4</b>
<b>2. Data Processor</b>	<b>4</b>
<b>3. General information on data processing</b>	<b>6</b>
<b>4. Data collected through the use of the app</b>	<b>11</b>
<b>5. Data processed when using the app</b>	<b>16</b>
<b>6. Sub-processors and infrastructure providers</b>	<b>26</b>
<b>7. Third-Party SDKs</b>	<b>35</b>
<b>8. Third parties</b>	<b>40</b>
<b>9. How we keep your data safe</b>	<b>40</b>
<b>10. Third party links</b>	<b>41</b>
<b>11. Updates to this privacy notice</b>	<b>41</b>

## 1. Data Controller

The data controller responsible for the purposes of the UK General Data Protection Regulation (UK GDPR) and other data protection regulations is Mission Aviation Fellowship UK, Charity Number 1064598, registered in England and Wales.

<b>Our support pages</b>	<a href="https://www.maf-uk.org/">https://www.maf-uk.org/</a>
<b>Email</b>	<a href="mailto:supporter.relations@maf-uk.org">supporter.relations@maf-uk.org</a>
<b>Post</b>	Castle House Castle Hill Avenue Folkestone, CT20 2TQ
<b>Telephone</b>	01303 852819

### Person with responsibility for data protection

MFC Community Sports has nominated a person with responsibility for data protection compliance within the business. You should contact them if you have any questions about the operation of this policy, if you need further information about the data protection legislation, or if you have any concerns that this policy is not being or has not been followed. They can be contacted as follows:

<b>Job Title</b>	Data Protection Officer
<b>Telephone Contact</b>	01303 852819
<b>Email</b>	<a href="mailto:dpo@maf-uk.org">dpo@maf-uk.org</a>

## 2. Data Processor

The data processor of the "MAF Wingmate app" responsible under the UK General Data Protection Regulation (UK GDPR) and other data protection regulations is If Give Limited, a registered company in England and Wales (Company Number 13889210). The contact details of the data processor are:

<b>Our support pages</b>	<a href="http://www.ifgive.app">www.ifgive.app</a>
<b>Email</b>	<a href="mailto:hello@ifgive.app">hello@ifgive.app</a>

<b>Post</b>	If Give Limited InfoLab21, Lancaster University, South Dr, Bailrigg Lancaster, Lancashire, LA1 4WA, United Kingdom
<b>Telephone</b>	+44 (0) 1524 88 48 18

### **Data Protection Officer**

If Give Limited has nominated a person with responsibility for data protection compliance within the business. You should contact them if you have any questions in regards to the processing of your data:

<b>Name</b>	Mike Harding
<b>Job Title</b>	Chief Data Officer
<b>Email</b>	mike@ifgive.app
<b>Post</b>	If Give Limited, Data Protection Officer, InfoLab21, Lancaster University, South Dr, Bailrigg Lancaster, Lancashire, LA1 4WA, United Kingdom
<b>Telephone</b>	+44 (0) 20 351 465 57

### **Sub-processors**

If Give Limited engages and appoints sub-processors (the list of which is available in [section 6](#)) to assist in the processing of data on behalf of the organisation. By utilising our services, you acknowledge and agree to the involvement of these sub-processors in handling the data under our established privacy and security standards.

## 3. General information on data processing

Below, we provide you with general information regarding the processing of your personal data when using the MAF Wingmate app (referred to below as the 'app').

It is important to understand that the collection and use of your personal data will depend on how you interact with us or the services you use. We only collect, use or share your personal data under Art. 6(1) (a) UK GDPR, Art 6(1) (b) UK GDPR, where we have a legitimate purpose and a legal basis for doing so.

### 3.1 What do we mean by 'legal basis'?

**Summary:** *We only process your personal information when we believe it is necessary and we have a valid legal reason (called legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfil our contractual obligations, to protect your rights, or to fulfil our legitimate business interests. Sections 5, 6, 7, and 8 outline the particular legal basis to process specific information.*

**Consent** under Art. 6(1) (a) UK GDPR: You have given the Data Controller your consent to process your personal data for the specific purpose explained to you. You have the right to withdraw your consent at any time. To do so please contact the Data Controller via the details supplied above.

**Contract** under Art 6(1) (b) UK GDPR: Data needed to fulfil a contract you have with the Data Controller. Alternatively, it's necessary to use your data because the Data Controller, or the Data Provider on behalf of the Data Controller, has asked you to do so, or you have taken specific steps before entering that contract.

**Legal Obligation** under Art 6(1) (c) UK GDPR: Use of your data is needed to comply with the law.

**Vital Interests** under Art 6(1) (d) UK GDPR: Processing of your data is necessary to protect your vital interests or those of another person. For example, to prevent you from serious physical harm.

**Public Task** under Art 6(1) (e) UK GDPR: Use of your data is necessary for the performance of a task carried out in the public interest, or because it is covered by a task set out in law, for example, for a statutory function.

**Legitimate Interests** under Art 6(1) (f) UK GDPR: Processing your data is necessary to support a legitimate interest the Data Controller or another party has, only where this is not outweighed by your own interests.

Please note that we may be unable to provide you with our app if you do not provide some of the data requested where your data is processed under the performance of a contract or for a legal obligation

### **3.2 Data sharing and international transfers**

**Summary:** *We may transfer, store, and process your information in countries other than your own. Sections 6, 7, and 8 outline more detailed information on data sharing and international transfers.*

As explained throughout this Privacy Policy, our data processor uses a number of services and sub-processors (see section 6 and 7) to help us deliver the app and keep your data secure. To provide the app and/or its services, it is necessary for us to share some of your personal data with them.

Where your personal data is shared outside the UK, we ensure that your personal data is given an equivalent level of protection, either because the jurisdiction to which your data is transferred has an 'adequate' data protection standard according to the UK Government, or by using another safeguard including the European Commission's Standard Contractual Clauses for transfers of personal information between our group companies, and between us and our third-party providers as well as other contractual agreements i.e. International Data Transfer Agreement (IDTA). These clauses require all recipients to protect all personal information that they process originating from the EEA or UK under equivalent UK/European data protection standards and regulations.

You can request a copy of such contractual agreement concluded with our service providers by emailing [data@ifgive.app](mailto:data@ifgive.app) or contacting If Give Limited through any of the contact details provided above. We have implemented similar appropriate safeguards

with our third-party service providers and partners and further details can be provided upon request.

### 3.3 Your rights

**Summary:** Under UK GDPR, you have rights to your data. You can request information, correct, limit, or delete it. You can also get your data in a readable format and complain to the UK Information Commissioner's Office (ICO) if you are unhappy with its handling.

When your personal data is processed, you are a data subject within the meaning of the UK GDPR and have the following rights:

#### 3.3.1. Right of access (Art. 15 UK GDPR)

You may request the data controller to confirm whether your personal data is processed by them. If such processing occurs, you can request the following information from the data controller:

- Purposes of processing
- Categories of personal data being processed.
- Recipients or categories of recipients to whom the personal data have been or will be disclosed. Planned storage period or the criteria for determining this period
- The existence of the rights of rectification, erasure restriction or opposition.
- The existence of the right to complain with a supervisory authority.
- If applicable, the origin of the data (if collected from a third party).
- If applicable, the existence of automated decision-making including profiling with meaningful information about the logic involved, the scope and the effects to be expected.
- If applicable, transfer of personal data to a third country or international organisation.

#### 3.3.2. Right to rectification (Art. 16 UK GDPR)

You have a right to rectification and/or modification of the data if your processed personal data is incorrect or incomplete. The data controller must correct the data without delay



### **3.3.3. Right to the restriction of processing (Art. 18 UK GDPR)**

You may request the restriction of the processing of your personal data under the following conditions:

- If you challenge the accuracy of your personal data for a period that enables the data controller to verify the accuracy of your personal data.
- The processing is unlawful, and you oppose the erasure of the personal data and instead request the restriction of their use.
- The data controller or its representative no longer needs the personal data for processing, but you need it to assert, exercise or defend legal claims; or
- If you have objected to the processing pursuant and it is not yet certain whether the legitimate interests of the data controller override your interests.

### **3.3.4. Right to erasure ("Right to be forgotten") (Art. 17 UK GDPR)**

If you request from the data controller to delete your personal data without undue delay, they are required to do so immediately if one of the following applies:

- Personal data concerning you is no longer necessary for the purposes for which they were collected or processed.
- You withdraw your consent on which the processing is based and where there is no other legal basis for processing the data.
- You object to the processing of the data and there are no longer overriding legitimate grounds for processing, or you object under Art. 21 (2) UK GDPR.
- Your personal data has been processed unlawfully.
- The personal data must be deleted to comply with a legal obligation in Union law or Member State law to which the data controller is subject.
- Your personal data was collected in relation to information society services offered under Art. 8 (1) UK GDPR.

**The right to deletion does not exist if the processing is necessary:**

- to exercise the right to freedom of speech and information;

- to fulfil a legal obligation required by the law of the Union or Member States to which the data controller is subject, or to perform a task of public interest or in the exercise of public authority delegated to the representative;
- for reasons of public interest in the field of public health;
- for archival purposes of public interest, scientific or historical research purposes, for statistical purposes; or
- to enforce, exercise or defend legal claims.

### **3.3.5. Right to data portability**

You have the right to receive the personal data you have provided to the data controller in a structured and machine-readable format. In addition, you have the right to transfer this data to another person without hindrance by the data controller who was initially given the data.

### **3.3.6. Right to object**

For reasons that arise from your particular situation, you have, at any time, the right to object to the processing of your personal data under Art. 6 (1) (e) or 6 (1) (f) UK GDPR; this also applies to profiling based on these provisions.

If the personal data relating to you are processed for direct marketing purposes, you have the right to object at any time to the processing of your personal data regarding such advertising; this also applies to profiling in association with direct marketing.

### **3.3.7. Right to complain to a supervisory authority**

You have the right to complain to the ICO if you are unhappy with how we have used your data and/or believe that the processing of the personal data concerning you violates the applicable law. We would welcome the opportunity to address your concerns before you approach the ICO and ask that you contact us in the first instance.

<b>Support pages</b>	<a href="http://www.ico.org.uk">www.ico.org.uk</a>
<b>Email</b>	<a href="mailto:info@ico.org.uk">info@ico.org.uk</a>
<b>Post</b>	Information Commissioner's Office Office Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom
<b>Telephone</b>	+44 (0) 303 123 1113

## 4. Data collected through the use of the app

### 4.1 Personal information you disclose to us

*Summary: We collect personal information that you provide to us during registration and when you activate or use specific features in the app (e.g. adding a payment card, or adding Gift Aid to your donation).*

We collect personal information that you willingly share with us when you register with the services, express an interest in obtaining information about us or our products and services when you participate in activities on the services, or otherwise when you contact us, our data processor, or the DPO of our data processor.

#### 4.1.1 Personal information provided by you

The personal information that we collect depends on the context of your interactions with us and the services, the choices you make, and the products and features you use. The personal information we collect may include the following:

- **Name**

**Data collected:** First name, Last name (required)

**Purpose:** App functionality, Developer communications, fraud prevention, security and compliance, advertising or marketing, account management

- **Email address**

**Data collected:** Email address (required)

**Purpose:** App functionality, developer communications, advertising or marketing, account management

- **User ID address**

**Data collected:** Automatically generate UUID4 identifier (required)

**Purpose:** App functionality, analytics, account management

- **Address**

**Data Collected:** Street, Postcode, Town/City, Country (optional)

**Purpose:** Gift Aid (App functionality, fraud prevention, security and compliance)

- **Contact preferences (email, push notifications)**

**Data Collected:** Optional

**Purpose:** App functionality, developer communications, fraud prevention, security and compliance, advertising or marketing, account management

#### **4.1.2 Sensitive Personal Information (Special Category Data)**

The app does not process sensitive information, also called special category data, as defined in Article 9 of the UK GDPR.

#### **4.1.3 Information on minors or other vulnerable groups**

We do not knowingly collect data from or market to individuals under 18 years of age or other vulnerable groups. By agreeing to the apps EULA, you confirm you are at least 18 years old. Should we discover personal information from users under 18, we will aim to deactivate the account and promptly remove such data from our records. If you know of any data collected from children under 18, please get in touch.

#### **4.1.4 Payment Details**

We may collect data necessary to process your payment if you make donations, such as your payment card number, and the security code associated with your payment method. The personal information we collect may include the following:

- **Name**

**Data collected:** First name, Last name (required)

**Purpose:** App functionality, Developer communications, fraud prevention, security and compliance, advertising or marketing, account management

- **Address**

**Data Collected:** Postcode, Address line, Town/City

**Purpose:** Gift Aid, Fraud prevention, security and compliance

- **Debit/credit card numbers**

**Data Collected:** Payment details (managed by Stripe Inc)

**Purpose:** App functionality, fraud prevention, security and compliance, account

management

All payment data is stored by Stripe. If you would like to contact Stripe, please use the contact details below:

<b>Support pages</b>	<a href="https://support.stripe.com">support.stripe.com</a>
<b>Email</b>	<a href="mailto:support.stripe.com/contact/email">support.stripe.com/contact/email</a>
<b>Post</b>	Stripe Technology Europe Ltd, The One Building 1, Lower Grand Canal Street, Dublin 2, Ireland
<b>Privacy Policy</b>	<a href="https://stripe.com/gb/privacy">stripe.com/gb/privacy</a>

If you make payments using Google Pay, your payment details are also processed by the European operating company of Google. If you would like to contact Google, please use the contact details below:

<b>Support pages</b>	<a href="https://support.google.com/googlepay">support.google.com/googlepay</a>
<b>Post</b>	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
<b>Privacy Policy</b>	<a href="https://support.google.com/googlepay/answer/10223752">support.google.com/googlepay/answer/10223752</a>

If you make payments using Apple Pay, your payment details are also processed by Apple Inc. If you would like to contact Apple, please use the contact details below:

<b>Support pages</b>	<a href="https://support.apple.com/en-gb/apple-pay">support.apple.com/en-gb/apple-pay</a>
<b>Post</b>	Apple Incorporated, One Apple Park Way, Cupertino, CA 95014, United States
<b>Privacy Policy</b>	<a href="https://support.apple.com/en-gb/HT203027">support.apple.com/en-gb/HT203027</a>

#### 4.1.5 Application Data

This information is primarily needed to maintain the security and operation of our application, for troubleshooting, and for our internal analytics and reporting purposes. If

you use our app, we also may collect the following information if you choose to provide us with access or permission:

- **Mobile Device Data**

**Data Collected:** Device information (such as your mobile device ID, model, and manufacturer), operating system, version information and system configuration information, device and application identification numbers, browser type and version, hardware model, and Internet Protocol (IP) address

**Purpose:** App functionality, fraud prevention, security and compliance, account management, analytics, service Improvement

We may request to send you push notifications regarding your account or certain features of the application. If you wish to opt-out from receiving these types of communications, you may turn them off in the app under More/Notification Settings:

- **Notifications**

**Data Collected:** Firebase messaging ID

**Purpose:** App functionality, communication, account management

## 4.2 Information automatically collected through the app

**Summary:** *Some information – such as your Internet Protocol (IP) address and/or browser and device characteristics – is collected automatically when you visit our services.*

If you allow us to, we automatically collect certain information when you visit, use, or navigate the services. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your pseudo-anonymised user identifier, IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our services, and other technical information. This information is primarily needed to maintain the security and operation of our services and for our internal analytics and reporting purposes. If you allow us to do so, we would also like to use some of this anonymised data for product improvement, data reporting, product development and non-commercial academic research.

## 4.2.1 App Information and Performance

### ■ Crash Logs

**Data Collected:** Data Collected: Logs are records that the application generates when it encounters an error or unexpected issue and subsequently terminates. For example, the number of times that the app has crashed, stack traces or information related to crashes (Optional)

**Purpose:** Analytics, Service Improvement

### ■ Diagnostics

**Data Collected:** Data gathered by the application to analyse its performance, identify potential issues, and improve overall functionality e.g. code warning or errors, loading time, latency, frame rate or technical diagnostics (Optional)

**Purpose:** Analytics, Service Improvement

## 4.2.2 App Activity

### ■ App Interactions

**Data Collected:** Data Collected: Information about how a user interacts with the app. For example, the number of times that they visit a page or what they tap on. (Optional)

**Purpose:** Analytics, service Improvement, academic research

## 4.2.3 Device or Other IDs

### ■ Device or Other IDs

**Data Collected:** Device ID, Firebase installation ID (Optional)

**Purpose:** Analytics, service Improvement, fraud prevention, security and compliance,

## 5. Data processed when using the app

**Summary:** We process your information to provide, improve, and administer our services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes (e.g. non-commercial academic research) with your consent. We keep your information for as long as necessary to fulfil the purposes outlined in this privacy notice unless otherwise required by law.

### 5.1 Overview

We process your personal information for a variety of reasons, depending on how you interact with our services, including:

- **To facilitate account creation and authentication and otherwise manage your account.** We process your information so you can create and log in to your account, as well as keep your account in working order.
- **To deliver and facilitate the delivery of services to you.** We process your information to provide you with the requested service.
- **To respond to user inquiries/offer you support.** We process your information to respond to your inquiries and solve any potential issues you might have with the requested service.
- **To send administrative information to you.** We may process your information to send you details about our products and services, changes to our terms and policies, and other similar information.
- **To protect our services.** We process your information as part of our efforts to keep our services safe and secure, including fraud monitoring and prevention.
- **To fulfil our legal obligations.** We may process your information when necessary as part of our legal obligations, for example, UK fundraising regulations, HMRC or other applicable laws and regulations.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm to vulnerable individuals.
- **To request your feedback.** We may process your information when necessary to request feedback and to contact you about your use of our services (optional).
- **To send you marketing and promotional communications.** We may process the personal information you send to us for our marketing purposes if this is following your marketing preferences (optional).



- **To identify usage trends.** We may process information about how you use our services to better understand how they are being used so we can improve them (optional).
- **To determine the effectiveness of our marketing and promotional campaigns.** We may process your information to better understand how to provide marketing and promotional campaigns that are most relevant to you (optional).
- **To detect technical issues or faults.** We may process your information, or anonymised/aggregated data as part of our efforts to keep our services operating, including bug fixing, availability monitoring and downtime prevention (optional).
- **To improve our service to you or create new products.** We may process anonymised and or aggregated information to improve our services or to create new products and services (optional).
- **Non-commercial academic research.** We may process anonymised data for non-commercial academic research and teaching purposes (optional).

During the use of the app, the following data is collected:

- **Personal Information**  
Data outlined in 4.1 and 4.2, may be collected during registration and app usage for various functionalities, communications, security measures, advertising, and account management.
- **Financial Information**  
Data outlined in 4.1.4, may be collected during card setup and payment transactions.
- **App Information and Performance**  
Data outlined in 4.2, in particular crash logs and diagnostics, may be collected optionally when errors occur or for performance analysis.
- **App Activity**  
App interactions and device/other IDs, as outlined in 4.1 and 4.2, are optionally collected during user engagement with the app. App usage is recorded optionally for diagnostics and service improvements and non-commercial academic research

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice unless a longer retention period is required or permitted by

law (such as tax, accounting, or other legal requirements). No purpose in this notice will require us to keep your personal information for longer than one hundred twenty (120) months past the termination of the user's account.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymise such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

## **5.2 Provision of app and creation of log files**

### **5.2.1. Description and scope of data processing**

Each time our app is accessed, our systems automatically collect some basic data and relevant information about the device accessing our services. The following data is collected:

- The device operating system and version
- Date and time of access
- IP Address
- This data is stored in the log files of our system.

### **5.2.2. Purpose of data processing**

Log files store data to maintain app functionality, optimise the app, and ensure the security of our services.

### **5.2.3. Legal basis for data processing**

The legal basis for the temporary storage of data and log files is Art. 6 (1) (f) UK GDPR.

### **5.2.4. Duration of storage**

The data will be deleted as soon as it is no longer necessary for its collection. The default retention period for the data is sixty (60) months.

### **5.2.5. Exercising your rights**

The collection of data for the provision of the app and the storage of the data in log files is necessary to ensure the security and operation of the app. You have the right to object to

these collections and their use Whether the objection is successful is to be determined within the framework of a balancing of interests.

## 5.3 App registration

### 5.3.1. Description and scope of data processing

We offer users the opportunity to register by providing personal data. The data is entered into an input mask transmitted to us and stored. The data will not be passed on to third parties. The following data is collected as part of the registration process:

- **Name**

**Data collected:** First name, Last name (required)

**Purpose:** App functionality, Developer communications, fraud prevention, security and compliance, advertising or marketing, account management

- **Email address**

**Data collected:** Email address (required)

**Purpose:** App functionality, developer communications, advertising or marketing, account management

- **IP**

**Data collected:** Your current IP address (required)

**Purpose:** App functionality, account management, fraud prevention,

- **Date and time of registration**

**Data collected:** Timestamp (required)

**Purpose:** App functionality, account management, analytics & monitoring

As part of the registration process, your consent to the processing of this data is obtained.

### 5.3.2. Purpose of data processing

User registration is necessary for the fulfilment of a contract with or for the execution of pre-contractual measures.

### 5.3.3. Legal basis for data processing

- The legal basis for data processing is Art. 6 (1) (a) UK GDPR where you have provided consent.

- The legal basis for the processing of registration data necessary to conclude or fulfil a contract with you is Art. 6 (1) (b) UK GDPR.
- The legal basis for the processing of registration data is Art 6(1) (c) UK GDPR where your data is needed to comply with the law is

#### **5.3.4. Duration of storage**

The data will be deleted as soon as it is no longer necessary to achieve the purpose for which it was collected.

This is the case for the data collected during the registration process for the fulfilment of a contract or the execution of pre-contractual measures if the data is no longer required for the implementation of the contract. Even after the conclusion of the contract, it may be necessary to store the personal data of the contractual partner to comply with contractual or legal obligations. The default storage duration for this data after account deletion is 72 months.

#### **5.3.5. Objection and removal**

You can cancel the registration at any time. The data above will only be processed upon successful registration. You have the right to request a change to the data stored about you at any time, through the following methods:

- You can configure and modify your data & privacy processing settings and how your data is collected and handled in the app under More/Privacy;
- You can edit your personal details (first and last name) in the app on the Profile page by tapping on "Edit your details";
- You can change your payment details on the Profile page by tapping on "Edit payment method";
- You can submit a request to delete certain data that we have collected through this app, without deleting your account;
- You can request to delete your entire account in the app

If the data is needed to fulfil a contract or for pre-contractual measures, deleting it prematurely is only possible if there are no contractual or legal obligations preventing its deletion.

## 5.4 Donation processing

### 5.4.1. Description and scope of data processing

You can donate through the app. The app supports payments through debit/credit cards, Google Pay and Apple Pay. We use payment service providers to process your payments, and you will be redirected to the payment provider upon clicking on "add card/change card". After completion of the payment process, we receive non-sensitive payment data (the last four digits of your card, the brand of your card, and the expiry date) from the payment service provider.

### 5.4.2. Payment Methods: Payment via credit card

If you choose to donate by credit card, payment details will be passed on to payment service provider Stripe for payment processing. Stripe complies with the requirements of the "Payment Card Industry (PCI) Data Security Standards" and has been certified by an independent PCI Qualified Security Assessor.

The following data will be transmitted regularly as part of payment via credit card:  
Purchase amount

- Date and time of purchase
- First and last name
- Address
- Email address
- Credit card number
- Credit card validity period
- Card validation code (CVC)

Payment data is passed on to the payment service provider Stripe Inc. The contact details for Stripe are below::

**Support pages**

[support.stripe.com](https://support.stripe.com)

**Email**

[support.stripe.com/contact/email](mailto:support.stripe.com/contact/email)

<b>Post</b>	Stripe Technology Europe, Limited, The One Building, 1, Lower Grand Canal Street, Dublin 2, Ireland
<b>Privacy Policy</b>	<a href="https://stripe.com/gb/privacy">stripe.com/gb/privacy</a>

### 5.4.3. Payment via Google Pay

It is possible to make payments via Google Pay. When you use Google Pay to conduct a transaction, Google collects information about the transaction, including the date, time and amount of the transaction, the merchant's location and description, a description provided by the seller of the goods or services purchased, any photo that you choose to associate with the transaction, the names and email addresses of the seller and buyer (or sender and recipient), the type of payment method used, your description of the reason for the transaction and the offer associated with the transaction, if any.

Further information on data processing by Google when making a payment via Google Pay can be found below:

<b>Support pages</b>	<a href="https://support.google.com/googlepay">support.google.com/googlepay</a>
<b>Contact</b>	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
<b>Privacy Policy</b>	<a href="https://support.google.com/googlepay/answer/10223752">support.google.com/googlepay/answer/10223752</a>

### 5.4.4. Payment via Apple Pay

It is possible to make payments via Apple Pay. When making a donation using Apple Pay, the following personal data is transferred to Apple: Postcode or equivalent information for tax and postage calculation.

- Merchant-specific account number.
- Postal address or email address
- Device-specific information, Apple ID, and location (if Location services for Wallet are enabled) for on-device fraud prevention assessments.
- Output of on-device fraud prevention assessments (not the underlying data).
- Postal address identifier for confirming address consistency across transactions.
- IP address (if available) for fraud prevention.

- Information about participating merchants associated with merchant-specific account numbers.

Further information on data processing by Apple when making a payment via Apple Pay can be found below:

<b>Support pages</b>	<a href="https://support.apple.com/en-gb/apple-pay">support.apple.com/en-gb/apple-pay</a>
<b>Contact</b>	Apple Incorporated, One Apple Park Way, Cupertino, CA 95014, United States
<b>Privacy Policy</b>	<a href="https://support.apple.com/en-gb/HT203027">support.apple.com/en-gb/HT203027</a>

#### **5.4.5. Purpose of data processing**

The transmission of payment data to payment service providers serves to process payments, e.g. if you purchase a product and/or use a service.

#### **5.4.6. Legal basis for data processing**

The legal basis for data processing is Art. 6 (1) (b) UK GDPR since the processing of the data is necessary for the execution of the contract we have with you.

#### **5.4.7. Duration of storage**

All payment data as well as data on possible chargebacks are only stored as long as they are required for payment processing and a possible processing of chargebacks and debt collection as well as for prevention of misuse. Furthermore, payment data may be stored beyond this if and as long as this is necessary to comply with statutory retention periods or to prosecute a specific case of misuse. Your personal data collected as part of a payment will be deleted at the end of the statutory retention period, i.e. after ten (10) years at the latest.

#### **5.4.8. Exercising your rights**

You can withdraw your consent to the processing of your payment data at any time by notifying the data controller or the payment service provider used. However, the payment

service provider used may still be required to process your payment data if and as long as this is necessary for the contractual payment processing or by law.

## **5.5 Contact via email**

### **5.5.1. Description and scope of data processing**

You can contact us via the email address provided on our app. In this case, your personal data transmitted with the email will be stored. The data will be used exclusively for the processing of the conversation.

### **5.5.2. Purpose of data processing**

If you contact us via email, this also constitutes the necessary legitimate interest in the processing of the data.

### **5.5.3. Legal basis for data processing**

The legal basis for the processing of data transmitted in the course of sending an email is Art. 6 (1) (f) UK GDPR. Our legitimate interest is to optimally answer your request that you send by email. If the purpose of the email contact is to conclude a contract, the additional legal basis for the processing is Art. 6 (1) (b) UK GDPR.

### **5.5.4. Duration of storage**

Email conversations with the sub-processor If Give Limited will be retained for as long as possible to provide a comprehensive and complete answer to your inquiry. Please refer to the privacy policy of Mission Aviation Fellowship UK for storage and retention of email conversations directly with Mission Aviation Fellowship UK.

### **5.5.5. Exercising your rights**

You can withdraw consent to the processing of your personal data at any time, by the following means:

- If you contact us by email, you can object to the storage of your personal data at any time. In this case, all personal data stored while establishing contact will be deleted.



## 5.6 App Performance Monitoring

### 5.6.1. Description and scope of data processing

If you consent, we process some elementary data in our app to monitor, analyse, and optimise system performance and resource utilisation. We use the following service providers to monitor and analyse app performance: Sentry (self-hosted) and PostHog (self-hosted).

### 5.6.2. Purpose of data processing

The collection, analysis and sharing of telemetry data serves in particular the following purposes:

- Infrastructure monitoring
- Application monitoring
- Resource optimization
- Bug fixing

### 5.6.3. Legal basis for data processing

The legal basis for data processing is Art. 6 (1) (a) UK GDPR where you have provided consent. The legal basis for the processing of registration data necessary to conclude or fulfil a contract with you is Art. 6 (1) (b) UK GDPR. The collection of this data is based on Art. 6(1)(f) UK GDPR. We have a legitimate interest in collecting the data necessary for app performance monitoring, analysis and optimisation.

### 5.6.4. Duration of storage

Your personal information will be stored as long as necessary to fulfil the purposes described in this Privacy Policy or as required by law.

### 5.6.5. Exercising your rights

You can object to the processing of your data by configuring the settings in Privacy Settings in the "More" section of the app, by sending an email to [data@ifgive.app](mailto:data@ifgive.app) or contacting If Give Limited through any of the contact details provided above.

## 6. Sub-processors and infrastructure providers

**Summary:** We use certified, GDPR-compliant sub-processors and infrastructure providers to offer our platform and services.

### 6.1 Content delivery network, provided by Cloudflare

**Summary:** This app uses Cloudflare Inc.'s services for security, performance, and reliability. Their data processing follows GDPR standards, mainly handling customer-controlled data. For secure data transfers, Cloudflare complies with the EU-U.S. Privacy Shield.

#### 6.1.1 Overview

We utilise Cloudflare, a US-based company specialising in security, performance, and reliability services globally, with multiple European offices. It ensures secure data transmission (SSL), enhances app performance via Content Delivery Network (CDN), protects against DDoS attacks, and fortifies security with the Web Application Firewall (WAF). Cloudflare may employ cookies for these services, and we've established a GDPR-compliant contract for data processing. For further GDPR-related details, visit Cloudflare's GDPR pages.

#### 6.1.2 Processed data

Cloudflare processes data based on what app operators control, varying with the services used. It doesn't retain customer content for popular services. Customers are responsible for their data compliance and transmissions. Most data in Cloudflare's network remains on their servers, with metadata processed in US and European data centres.

Log data regarding network events is maintained, containing minimal personal info like IP addresses, and processed for a limited time. For security, Cloudflare employs cookies like (`__cfduid`) to identify users and apply security settings, yet it doesn't store personal data and is necessary for security features.

Cloudflare collaborates with third-party providers under strict instructions, ensuring personal data isn't shared without explicit consent.

### **6.1.3 Legal basis**

The legal basis of the processing is your consent according to Art. 6 (1) (a) GDPR unless indicated differently in the different processing activities set out above. If you do not want Cloudflare to collect and process the aforementioned data, you can refuse your consent or withdraw it at any time with effect for the future.

### **6.1.4 Retention period**

Cloudflare retains data logs briefly, usually deleting them within 24 hours. Personal data like IP addresses isn't stored, but certain information is kept indefinitely for Cloudflare Resolver's performance and security identification purposes, detailed in their permanent logs. All collected data, temporary or permanent, undergoes a process to remove personal information. Cloudflare anonymises permanent logs. Their privacy policy states they aren't responsible for received content, directing inquiries about content updates or deletion to the app operator.

### **6.1.5 Third-country transfers**

The vast majority of data that transits Cloudflare's network stays on Cloudflare's Edge servers. Metadata about this activity is processed on behalf of the data controller in data centres in the United States and Europe. Cloudflare is an active participant in the EU-U.S. Privacy Shield Framework which regulates the correct and secure transfer of personal data. You can find more information at [www.privacyshield.gov/participant](http://www.privacyshield.gov/participant).

### **6.1.6 Provision mandatory or required**

The provision of your personal data is voluntary, based solely on your consent. If you prevent access, this can lead to functional limitations on the app.

### **6.1.7 Further inquiries or withdrawal of consent**

To prevent data collection and processing by Cloudflare when accessing websites provided by our sub-processor, you can deactivate script code execution or use a script blocker in your browser. You can also adjust your settings to prevent cookie storage, though it might limit app functions. To request data deletion please contact Cloudflare through one of the following methods:

**Support pages**

[support.cloudflare.com](https://support.cloudflare.com)

**Email**

[privacyquestions@cloudflare.com](mailto:privacyquestions@cloudflare.com)

**Post**

Cloudflare Incorporated  
101 Townsend St., San Francisco  
CA 94107, United States

**Privacy Policy**

[www.cloudflare.com/en-gb/trust-hub/gdpr/](https://www.cloudflare.com/en-gb/trust-hub/gdpr/)

## 6.2 Server and Database infrastructure, provided by OVH Cloud

### 6.2.1 Overview

OVHCloud is an appointed sub-processor to host the technical platform infrastructure for the app and affiliated services located in secure, ISO 27001-certified data centre facilities. We use OVHcloud as a subprocessor to host Service data and provide other infrastructure, including database servers, that helps with the delivery of the Service. OVH Cloud is a leading global cloud service provider that offers a wide range of cloud-based solutions, including hosting, dedicated servers, public and private cloud services, and related infrastructure and software services.

### 6.2.2 Processed data

All application data, including customer data, and end-user data for services provided by If Give Limited on their website (ifgive.app) or mobile applications on behalf of our customer.

### 6.2.3. Security Measures

We ensure that any data hosted and processed by OVH Cloud is subject to robust security measures to prevent unauthorised access, disclosure, or alteration of information. OVH Cloud complies with industry standards and is certified under [ISO 27001](#), [ISO 27017](#), [ISO 27018](#), [ISO 27701](#), [SecNumCloud \(private cloud\)](#), [HDS](#) and adheres to the EU GDPR.

### 6.2.4 Legal basis

The legal basis for data processing is Art. 6 (1) (a) UK GDPR where you have provided consent. The legal basis for the processing of registration data necessary to conclude or fulfil a contract with you is Art. 6 (1) (b) UK GDPR.

### 6.2.5 Retention period

OVH provides server and database capacities to If Give Limited. The retention period for data is outlined in sections 4 and 5 of this privacy policy. Under section 5.3.7 (Duration of Storage) your personal data will be deleted at the end of the statutory retention period, i.e. after 10 years at the latest.

### 6.2.6 Third-country transfers

If Give is using OVH infrastructure to replicate Customer Data between multiple geographically dispersed data centres operated by OVH Cloud in the UK and the European Economic Area (United Kingdom, France, Germany and Poland).

### 6.2.7 Provision mandatory or required

The provision of your data is required for the technical function of the app. If you prevent access, this can lead to functional limitations on the app.

### 6.2.8 Further inquiries or withdrawal of consent

OVHCloud is an appointed sub-processor of If Give Limited, providing technical infrastructure required for the operation of the app. Please reach out to our data processor If Give Limited for any queries related to the processing and storage of information or your withdrawal of consent. If you would like to get in touch with OVH or learn more about their data privacy and data security policy please use the contact details below:

<b>Support pages</b>	<a href="https://help.ovhcloud.com">help.ovhcloud.com</a>
<b>Post</b>	OVHcloud 2, Rue Kellermann, 59100 Roubaix, France, Phone: .
<b>Telephone</b>	+33 (0) 972 101 007

## 6.3 Cloudflare R2 Storage

### 6.3.1 Overview

We host some of our application data (e.g. images and asset resources) in ISO 27001-certified data centre facilities. Cloudflare R2, an S3-compatible, zero egress-fee, globally distributed object storage certified under ISO 27001 certified data centre facilities.

### **6.3.2 Processed data**

Non-personal data and resources such as images and assets for our website and mobile applications.

### **6.3.3 Security Measures**

We ensure that any data hosted and processed by Cloudflare is subject to robust security measures to prevent unauthorised access, disclosure, or alteration of information. Cloudflare complies with industry standards and is certified under [ISO 27001:2013](#), [ISO 27701:2019](#), [ISO 27018:2019](#), [SOC2](#), [PCI DSS 3.2.1](#), [C5:2020](#) and adheres to the EU GDPR.

### **6.3.4 Legal basis**

The legal basis for data processing is Art. 6 (1) (a) UK GDPR where you have provided consent. The legal basis for the processing of registration data necessary to conclude or fulfil a contract with you is Art. 6 (1) (b) UK GDPR.

### **6.3.5 Retention period**

Cloudflare retains data logs briefly, usually deleting them within 24 hours. Personal data like IP addresses isn't stored, but certain information is kept indefinitely for Cloudflare Resolver's performance and security identification purposes, detailed in their permanent logs.

### **6.3.6 Third-country transfers**

R2 buckets are restricted to the jurisdiction of the European Union to meet data residency requirements. Locations within the specified jurisdiction will be automatically chosen. Data may be distributed to the vast Cloudflare's distributed content delivery cache network across Cloudflare's Edge servers.

### **6.3.7 Provision mandatory or required**

The provision of your data is voluntary, based solely on your consent. If you prevent access, this can lead to functional limitations on the app.

### **6.3.8 Further inquiries or withdrawal of consent**

Cloudflare provides the core infrastructure required for the operation of the app. Please reach out to our data processor If Give Limited for any queries related to the processing

and storage of information or your withdrawal of consent. If you would like to get in touch with Cloudflare or learn more about their data privacy policy, see below:

<b>Support pages</b>	<a href="https://support.cloudflare.com">support.cloudflare.com</a>
<b>Email</b>	<a href="mailto:privacyquestions@cloudflare.com">privacyquestions@cloudflare.com</a>
<b>Post</b>	Cloudflare Incorporated 101 Townsend St., San Francisco CA 94107, United States

## 6.4 Google Firebase Cloud Messaging

### 6.4.1 Overview

Firebase, provided by Alphabet Inc., is used for Cloud Messaging, facilitating the efficient sending of push notifications to mobile and web applications.

### 6.4.2 Processed data

Firebase Cloud Messaging uses Firebase installation IDs to determine which devices to deliver messages to.

### 6.4.3 Security Measures

Firebase Cloud Messaging has deployed a series of security measures and undergone certification, including ISO 27001 and SOC 1, SOC 2, and SOC 3.

### 6.4.4 Legal basis

The legal basis for data processing is Art. 6 (1) (a) UK GDPR where you have provided consent to receive push notifications. The legal basis for the processing of Firebase installation IDs is Art. 6 (1) (b) to fulfil a legal contract with and under Art 6(1) (f)UK GDPR, a legitimate interest.

### 6.4.5 Retention period

Firebase retains Firebase installation IDs until the Firebase customer makes an API call to delete the ID. After the call, data is removed from live and backup systems within 180 days.

### **6.4.6 Third-country transfers**

Standard Contractual Clauses as the approved legal mechanism for transferring relevant data under the GDPR. These Clauses, approved by the European Commission on June 4, 2021, are integrated into the contractual agreements with Firebase to facilitate data transfers from the EEA, UK, or Switzerland to the United States and other locations.

### **6.4.7 Provision mandatory or required**

The provision of notification IDs is primarily based on your consent. If you prevent access, this can lead to functional limitations on the app (i.e. we won't be able to inform you about updates to your pledges using push notifications).

### **6.4.8 Further inquiries or withdrawal of consent**

You are free to disable notifications on an operating system level (the instructions differ between iOS and Android), or to configure when and how we are allowed to send you notifications (e.g in the overview page for each pledge and within the app settings under "More, Notification settings". For additional information please refer to Google Firebase Privacy policy.

#### **Privacy Policy**

[firebase.google.com/support/privacy](https://firebase.google.com/support/privacy)

#### **Post**

Alphabet Incorporated  
600 Amphitheatre Parkway, Mountain View,  
CA 94043, United States

## **6.5 Google Cloud email relay**

### **6.5.1 Overview**

The app uses Google Cloud (Alphabet Inc) email relay service for secure and dependable email delivery to you. All emails are encrypted and utilise robust security measures including Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).



### **6.5.2 Processed data**

Sender and recipient email address, time and subject of email, a message ID, the delivery status as well as the IP address of the sender and recipient servers.

### **6.5.3 Security Measures**

ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 2/3

### **6.5.4 Legal basis**

The legal basis for the processing of personal data (i.e. recipient / your email address) is Art. 6 (1) (b) to fulfil a legal contract with and under Art 6(1) (f)UK GDPR our legitimate business interest.

### **6.5.5 Retention period**

Data is retained through Google's Email log search for 30 days.

### **6.5.6 Third-country transfers**

Data is processed under UK/EU data processing law on servers located in the European Union.

### **6.5.7 Provision mandatory or required**

The provision of your data is required for the technical function of the app. If you prevent access, this can lead to functional limitations (e.g. prevent you to register or login) on the app.

### **6.5.8 Further inquiries or withdrawal of consent**

For additional information please refer to Google Cloud Privacy policy.

#### **Privacy Policy**

[cloud.google.com/terms/cloud-privacy-notice](https://cloud.google.com/terms/cloud-privacy-notice)

#### **Post**

Alphabet Incorporated  
600 Amphitheatre Parkway, Mountain View,  
CA 94043, United States

## **6.6 GetAdress (Address Lookup)**

### **6.6.1 Overview**

To lookup addresses when you setup Gift Aid, the app is using a third party service called getAddress.io to receive the address details of a postcode you provide. The postcode you provide is shared with the service provider, however, no personal information about yourself is shared.

### **6.6.2 Processed data**

The postcode you provide when creating a Gift Aid declaration.

### **6.6.3 Legal basis**

The legal basis for the processing and sharing the postcode you provide is Art. 6 (1) (b) to fulfil a legal contract with and under Art 6(1) (f)UK GDPR, a legitimate interest of our business to capture valid addresses.

### **6.6.4 Retention period**

Besides the postcode provided, the third party will not collect any personal information about yourself and is unable to link the postcode to you as an individual. We will collect and store the address information used to process Gift Aid for a minimum period of seventy two (72) months to comply with legal requirements, but no longer than one hundred and twenty (120) months.

### **6.6.5 Third-country transfers**

Personal data will not be transferred to countries outside of the UK/EEA.

### **6.6.6 Provision mandatory or required**

The provision of a postcode (and your address)

### **6.6.7 Further inquiries**

The provision of a postcode (and your address)

**Privacy Policy**

[getaddress.io/privacypolicy](https://getaddress.io/privacypolicy)

**Post**

Codeberry Limited  
2 Askham Row Benwick Road  
March, England, PE15 0WN

## **7. Third-Party SDKs**

### **7.1 Sentry**

#### **7.1.1 Overview**

The Sentry SDK, developed by Functional Software, Inc., is designed for error-monitoring software applications. It captures and reports errors, exceptions, and crashes in real-time, allowing developers to identify and address issues quickly. The SDK enhances the debugging process and contributes to improving the overall stability and reliability of applications. Data collected is collected on self-hosted servers by If Give Limited and not shared with the SDK manufacturer.

#### **7.1.2 Processed data**

Non-personal data and resources such as images and assets for our website and mobile applications.

#### **7.1.3 Legal basis for data processing**

The legal basis for data processing is Art. 6 (1) (a) UK GDPR where you have provided consent. The legal basis for the processing of registration data necessary to conclude or fulfil a contract with you is Art. 6 (1) (b) UK GDPR. The collection of this data is based on Art. 6(1)(f) UK GDPR. We have a legitimate interest in collecting the data necessary for app performance monitoring, analysis and optimisation.

#### **7.1.4 Retention**

Your personal information will be stored as long as necessary to fulfil the purposes described in section 4.2.

### **7.1.5 Third-country transfers**

The Sentry installation used for the app and services is “Self-Hosted” by If Give Limited. Data is only processed in the United Kingdom and the European Economic Area by the data processor If Give Limited in infrastructure provided by OVHCloud. The data is not shared with any third parties.

### **7.1.6 Withdrawal of consent**

You have the right to revoke your declaration of consent under data protection law at any time. The revocation of the consent does not affect the lawfulness of the processing carried out based on the consent up to the revocation. You can manage their consent preferences for data processing by Sentry SDKs by navigating to “More” and selecting “Privacy” within the app. Opt-out options are available in these sections. Please contact the data processor If Give Limited (contact details above) for further information. You can also object to the processing of your data by sending an email to [data@ifgive.app](mailto:data@ifgive.app) or contacting If Give Limited through any of the contact details provided above.

### **7.1.7 Contact the SDK manufacturer**

You can contact the SKD manufacturer and read more about their privacy policy below.

<b>Privacy Policy</b>	<a href="https://sentry.io/privacy">sentry.io/privacy</a>
<b>Post</b>	Functional Software, Inc 45 Fremont Street, 8th Floor, San Francisco, CA 94105, United States

## **7.2 Firebase SDK**

### **7.2.1 Overview**

Firebase SDK, developed by Alphabet Inc., is used for Cloud Messaging, facilitating the efficient sending of push notifications to mobile and web applications and App Check, a feature designed to enhance the security of these applications by protecting against abuse and unauthorised access. Firebase App Check helps ensure that only genuine, authorised instances of the app interact with the provided services, contributing to a more secure and reliable user experience.

### **7.2.2 Processed data**

Firebase Cloud Messaging uses Firebase installation IDs to determine which devices to deliver messages to. Firebase App Check uses attestation material required by the corresponding attestation provider and received from end-users devices to help establish the integrity of the device and/or the app. Attestation materials are sent to the corresponding attestation provider for validation based on the developer's configuration. App Check tokens obtained from successful attestations are sent with every request to supported Firebase services to access resources protected by App Check.

### **7.2.3 Legal basis**

The functionalities provided by SDKs are strictly necessary to provide the basic services of the app-based and processed under Art. 6 (1) (b) UK GDPR to fulfil a contract with you and legitimate interests under Art. 6 (1) (f) UK GDPR.

### **7.2.4 Retention**

Attestation material is not retained by Firebase App Check, but when it is sent to attestation providers, it is subject to the terms of those attestation providers. App Check tokens returned from successful attestations are valid throughout their Time-To-Live (TTL) duration, which cannot be longer than 7 days. For developers who use replay protection features, App Check stores the App Check tokens used with these features for at most 30 days. Other App Check tokens not used with replay protection features are not retained by Firebase services.

### **7.2.5 Third country transfers**

Standard Contractual Clauses as the approved legal mechanism for transferring relevant data under the GDPR. These Clauses, approved by the European Commission on June 4, 2021, are integrated into the contractual agreements with Firebase to facilitate data transfers from the EEA, UK, or Switzerland to the United States and other locations.

### **7.2.6 Withdrawal of consent**

You can manage their consent preferences for data processing by Sentry SDKs by navigating to "More" and selecting "Privacy" within the app. Opt-out options are available

in these sections. Please contact the data processor If Give Limited (contact details above) for further information. The use of App Check is a requirement for the functional operability of the app, withdrawal of consent will impact the ability of the app to function as intended.

### **7.2.7 Further inquiries or withdrawal of consent**

You can contact the SDK manufacturer and read more about their privacy policy below.

**Privacy Policy**

[firebase.google.com/support/privacy](https://firebase.google.com/support/privacy)

**Post**

Alphabet Incorporated  
600 Amphitheatre Parkway, Mountain View,  
CA 94043, United States

## **7.3 PostHog**

### **7.3.1 Overview**

The PostHog SDK, from PostHog Inc., is employed for product analytics and feature tracking. It enables developers to understand user behaviour, track feature usage, and gather insights into how users interact with an application. The SDK supports data-driven decision-making and aids in optimising the user experience based on usage patterns. Data collected is collected on self-hosted servers by If Give Limited and not shared with the SDK manufacturer.

### **7.3.2 Processed data**

Events and Interactions: It's data about what users do in an app – like clicks, page views, using features, or how they interact with different parts. User Attributes: This is all about users—stuff like who they are (user IDs or emails), their age, where they're from, or how they behave online.

### **7.3.3 Legal basis for data processing**

The legal basis for data processing is Art. 6 (1) (a) UK GDPR where you have provided consent. The legal basis for the processing of registration data necessary to conclude or fulfil a contract with you is Art. 6 (1) (b) UK GDPR. The collection of this data is based on Art. 6(1)(f) UK GDPR. We have a legitimate interest in collecting the data necessary for app performance monitoring, analysis and optimisation.

### **7.3.4 Retention**

Your personal information will be stored as long as necessary to fulfil the purposes described in section 4.2.

### **7.3.5 Third-country transfers**

The Sentry installation used for the app and services is "Self-Hosted" by If Give Limited. Data is only processed in the United Kingdom and the European Economic Area by the data processor If Give Limited in infrastructure provided by OVHCloud. The data is not shared with any third parties.

### **7.3.6 Withdrawal of consent**

You have the right to revoke your declaration of consent under data protection law at any time. The revocation of the consent does not affect the lawfulness of the processing carried out based on the consent up to the revocation. You can manage their consent preferences for data processing by PostHogs SDKs by navigating to "More" and selecting "Privacy" within the app. Opt-out options are available in these sections. Please contact the data processor If Give Limited (contact details above) for further information. You can also object to the processing of your data by sending an email to [data@ifgive.app](mailto:data@ifgive.app) or contacting If Give Limited through any of the contact details provided above.

### **7.1.7 Contact the SDK manufacturer**

You can contact the SKD manufacturer and read more about their privacy policy below.

**Privacy Policy**

[posthog.com/privacy](https://posthog.com/privacy)

**Post**

PostHog Incorporated  
Market Street 4008,  
San Francisco, CA 94114, United States

## 8. Third parties

**Summary:** *We may share information in specific situations described in this privacy policy and/or with the following third parties.*

**In addition to how we treat your information outlined in section 4,5, 6 and 7, we may also need to share your personal information in the following situations:**

**Legal requirement:** We may share your information with government bodies or agencies (for example HMRC) to remain compliant with legislation, or if they request this data as part of an inquiry or legal proceedings.

**Business Transfers:** We may share or transfer your information in connection with or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

**Affiliates:** We may share your information with our affiliates, in which case we will require those affiliates to honour this privacy notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us.

**Business Partners:** We may share your information with our business partners to offer you certain products, services, or promotions.

## 9. How we keep your data safe

**Summary:** *We aim to protect your personal information through a system of organisational and technical security measures.*

Our data processors have implemented appropriate and reasonable technical and organisational security measures designed to protect the security of any personal information processed in the app, including UK Cyber Essentials and Cyber Assurance Level 1 Certification of the Certification and Information Assurance for Small and Medium Enterprises Consortium. However, it is important to recognise that no transmission over the internet nor storage technology can be guaranteed to be 100% secure. Despite our efforts, we cannot assure that hackers, cybercriminals, or unauthorised third parties will not breach our security and access or manipulate your information.



## 10. Third party links

**Summary:** *Our app may include links to third-party websites for which we take no responsibility.*

Our app may, from time to time, contain links to third party websites (such as the websites of partner networks, advertisers and affiliates). If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

## 11. Updates to this privacy notice

**Summary:** *Yes, we will update this notice as necessary to stay compliant. We will inform all users if these changes happen.*

We may update this privacy notice from time to time. The updated version will be indicated by an updated 'Revised' date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information.