

PerfectWiFi PRIVACY POLICY – UNITED KINGDOM

Version: 1.0 Effective date: 9 August 2026

1. DATA CONTROLLER

The data controller responsible for personal data processed in connection with the use of the PerfectWiFi application is:

Łukasz Gnoiński Address: Leszczynowa 42, 05-090 Laszczki, Poland Email: support@sidekickaimanager.app

For matters relating to personal data protection, privacy, or the exercise of data protection rights, users may contact the Data Controller at the email address above.

This Privacy Policy applies in particular to users located in the United Kingdom.

The Data Controller processes personal data in accordance with applicable UK data protection law, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and, where applicable to electronic communications and access to information stored on users' devices, the Privacy and Electronic Communications Regulations 2003 (PECR), as amended.

1. SCOPE OF THIS PRIVACY POLICY

This Privacy Policy describes how personal data is processed in connection with the use of the PerfectWiFi mobile application on Android devices by users in the United Kingdom.

The application is designed to:

- analyse WiFi network quality;
- measure signal strength;
- test internet connection speed;
- analyse basic local network parameters;
- help plan the optimal placement of routers and network devices;
- visualise predicted WiFi coverage.

• HOW THE APPLICATION WORKS

PerfectWiFi operates primarily locally on the user's device.

The application does not require the user to create an account and does not maintain its own central server for storing users' measurement data.

The application may provide the following functionality:

- real-time WiFi signal strength measurement;
- scanning of WiFi networks and devices on the local network;
- internet connection speed testing;
- analysis of basic router and connection information;

- recording of signal measurement routes;
 - importing a floor plan as an image or PDF file;
 - local analysis of wall placement;
 - recommendations for optimal router and mesh device placement;
 - generation of predicted WiFi coverage maps;
 - export of results to PDF files.
- DATA PROCESSED LOCALLY

The following data is processed exclusively locally on the user's device and is not transmitted to the Data Controller as part of a centrally stored user database:

- WiFi network scan results;
- network identifiers (SSID/BSSID);
- signal strength levels;
- lists of devices detected on the local network;
- local IP addresses of devices;
- MAC addresses of devices;
- device names assigned by the user;
- measurement history;
- recorded measurement routes;
- photographs and PDF files containing floor plans;
- results of local image analysis;
- placement of routers, mesh devices and walls;
- generated PDF files.

This data remains on the user's device until deleted by the user, removed through the device or application settings, or deleted as a result of uninstalling the application.

The Data Controller does not use locally stored measurement data to create a central user profile.

1. ANDROID SYSTEM PERMISSIONS

The application may request or use the following Android system permissions:

5.1. Location Access – ACCESS_FINE_LOCATION

Android may require this permission for certain WiFi scanning functionality.

The application does not use GPS location data to track the user's movements unless a specific application feature expressly requires information associated with a measurement route.

Granting a system permission does not in itself mean that the Data Controller receives or stores the user's GPS location history.

5.2. Nearby WiFi Devices – NEARBY_WIFI_DEVICES

This permission may be used to obtain information about nearby WiFi networks and devices on supported versions of Android.

5.3. WiFi State – ACCESS_WIFI_STATE

This permission allows the application to read information about the current WiFi connection and its parameters.

5.4. Change WiFi State – CHANGE_WIFI_STATE

This permission allows the application to initiate WiFi-related operations, including network scanning where supported by the Android operating system.

5.5. Network State – ACCESS_NETWORK_STATE

This permission allows the application to determine whether a network connection is available.

5.6. Internet Access – INTERNET

Internet access may be used for:

- performing internet speed tests;
- retrieving information about the user's public IP address;
- identifying the user's internet service provider;
- displaying advertisements in the free version of the application;
- processing subscription purchases.

5.7. Activity Recognition – ACTIVITY_RECOGNITION

This permission may be used to measure movement or distance travelled when the user uses the application's measurement route functionality.

1. DATA SHARED WITH THIRD PARTIES

The application uses certain third-party technology and service providers.

Depending on the particular service and processing activity, a third-party provider may act as an independent controller or as a processor on behalf of the Data Controller.

6.1. Google AdMob

The free version of the application may display advertisements through Google AdMob.

Depending on the user's privacy settings and applicable consent requirements, Google may process information including:

- the device's advertising identifier;
- technical information about the device;
- information concerning advertising activity;
- information about interactions with advertisements;
- information relating to advertising and privacy settings.

Where technologies used for advertising store information on, or access information already stored on, the user's device, the applicable requirements of PECR may apply.

The Data Controller will not treat this Privacy Policy alone as evidence that the user has consented to optional advertising technologies where separate consent is legally required.

6.2. Google User Messaging Platform (UMP)

Google User Messaging Platform may be used to manage privacy settings and consent relating to advertising.

It may process information including:

- the user's consent status;
- advertising preferences;
- technical information required to operate the consent mechanism;
- information concerning the user's approximate region.

Where consent is required by applicable law, it will be requested through an appropriate consent mechanism.

6.3. Google Play Billing

Subscriptions and in-app purchases are processed through Google Play.

The Data Controller does not receive the user's full payment card details.

Google may process transaction-related information in accordance with its own privacy policy and the applicable Google Play terms.

6.4. Cloudflare Speed Test

When the user performs a speed test, the device may connect to speed.cloudflare.com.

Cloudflare may process the device's IP address and technical information necessary to perform the speed test.

6.5. ipify

The ipify service may be used to display the user's public IP address.

For this purpose, the user's public IP address may be processed by the service.

6.6. RDAP / RIPE NCC

RDAP / RIPE NCC services may be used to identify the user's internet service provider (ISP) based on the public IP address.

For this purpose, the public IP address may be processed by the relevant service.

1. LEGAL BASES FOR PROCESSING

Where the Data Controller is subject to UK data protection law, personal data is processed in accordance with the UK GDPR and the Data Protection Act 2018.

Depending on the particular processing activity, the legal basis may include:

- Article 6(1)(b) UK GDPR – processing necessary for the performance of a contract with the user or for taking steps at the user's request prior to entering into a contract;
- Article 6(1)(c) UK GDPR – processing necessary for compliance with a legal obligation;
- Article 6(1)(a) UK GDPR – the user's consent;
- Article 6(1)(f) UK GDPR – processing necessary for the purposes of the legitimate interests pursued by the Data Controller, except where those interests are overridden by the user's interests or fundamental rights and freedoms.

Where processing requires consent under PECR, the required consent will be obtained in accordance with PECR and the applicable UK GDPR requirements.

1. ADVERTISING AND CONSENT

The free version of the application may display advertisements.

Certain technologies used to deliver, personalise, measure or otherwise support advertising may be subject to PECR requirements concerning the storage of information on, or access to information already stored on, the user's device.

Where prior consent is legally required, the relevant non-essential technology will not be used before the required consent has been obtained.

Where consent is required, it will be requested in a manner designed to ensure that it is freely given, specific, informed and unambiguous.

Users may withdraw consent through the privacy settings available within the application or through another mechanism provided for the relevant service.

Withdrawal of consent does not affect the lawfulness of processing carried out before consent was withdrawn.

1. SUBSCRIPTIONS

The application may offer optional automatically renewing subscriptions.

Purchases are processed through Google Play.

The Data Controller does not have access to users' payment card details and does not process card payments directly.

Information concerning:

- subscription prices;
- billing periods;
- automatic renewal;
- cancellation;

- refunds;

may also be governed by the applicable Google Play terms and policies.

1. INTERNATIONAL DATA TRANSFERS

Some third-party service providers used by the application may process personal data outside the United Kingdom.

Where a transfer constitutes a restricted transfer under the UK GDPR, the Data Controller will use an appropriate transfer mechanism permitted under UK data protection law.

Depending on the circumstances, this may include:

- UK adequacy regulations;
- the UK International Data Transfer Agreement (UK IDTA);
- the UK Addendum to the EU Standard Contractual Clauses, where applicable;
- another lawful transfer mechanism or safeguard recognised under UK data protection law.

Where required, the Data Controller may carry out an appropriate assessment of the level of protection provided by the transfer mechanism and the destination country.

1. DATA RETENTION

Data processed locally by the application remains on the user's device until:

- manually deleted by the user;
- the relevant files are deleted;
- application data is cleared;
- the application is uninstalled.

The Data Controller does not maintain a central database containing users' locally generated WiFi measurements.

Personal data processed by third-party service providers may be retained by those providers for periods determined by their own privacy policies, contractual arrangements and legal obligations.

The Data Controller seeks to retain personal data only for as long as necessary for the purposes for which it was collected, taking into account legal obligations, security requirements, dispute resolution and the establishment, exercise or defence of legal claims.

1. YOUR DATA PROTECTION RIGHTS IN THE UNITED KINGDOM

Depending on the circumstances, users may have rights under the UK GDPR and the Data Protection Act 2018, including:

- the right to be informed about the processing of personal data;
- the right of access to personal data;
- the right to rectification of inaccurate or incomplete personal data;
- the right to erasure in certain circumstances;
- the right to restriction of processing in certain circumstances;
- the right to data portability where the applicable conditions are met;

- the right to object to certain processing activities;
- the right to withdraw consent at any time where processing is based on consent;
- rights relating to certain decisions based solely on automated processing, where applicable.

Not every right applies in every situation. The availability of a particular right depends on the legal basis and circumstances of the relevant processing.

To exercise a data protection right, users may contact the Data Controller:

support@sidekickaimanager.app

The Data Controller may request information reasonably necessary to verify the identity of the person making the request.

1. RESPONSE TO DATA SUBJECT REQUESTS

The Data Controller will handle requests concerning data protection rights in accordance with the UK GDPR.

As a general rule, a valid request will be responded to without undue delay and normally within one month of receipt.

Where permitted by law, this period may be extended where a request is particularly complex or where the user has made multiple requests.

Where an extension is necessary, the user will be informed of the extension and the reasons for it.

Requests concerning data protection rights are generally free of charge. In circumstances permitted by law, the Data Controller may charge a reasonable fee or refuse to act on a request that is manifestly unfounded or excessive.

1. DATA PROTECTION COMPLAINTS

Users are encouraged to contact the Data Controller first if they have concerns about how their personal data is being processed.

Privacy and data protection complaints may be submitted to:

support@sidekickaimanager.app

The Data Controller will maintain an appropriate procedure for handling complaints concerning personal data processing.

If the user remains dissatisfied with the response or believes that their personal data has been processed in breach of applicable data protection law, the user may lodge a complaint with the Information Commissioner's Office (ICO), the UK's independent supervisory authority for data protection.

Information about how to make a complaint to the ICO is available at:

<https://ico.org.uk/make-a-complaint/data-protection-complaints/>

1. DATA SECURITY

The Data Controller implements appropriate technical and organisational measures designed to protect personal data against unauthorised access, accidental loss, destruction, alteration or disclosure.

A key privacy feature of the application is that the majority of data generated by WiFi measurements and network analysis is processed locally on the user's device.

The Data Controller does not operate a central repository containing users' locally generated WiFi scan results.

Users should nevertheless be aware that information stored on their device may be accessible to persons who have access to the device, its backups or its sharing functionality.

1. EXPORTING PDF FILES

PDF files generated by the application may contain information concerning WiFi networks, devices, measurements or floor plans.

Such files are transferred through the Android system sharing mechanism only when the user chooses to share them.

Once a file has been shared with another application, service or person, subsequent processing may be governed by that recipient's own privacy policy and practices.

The Data Controller does not control the subsequent use of a file after the user voluntarily shares it.

1. CHILDREN

The application is not directed at children under the age of 13.

The Data Controller does not knowingly seek to collect personal data from children in a manner that would breach applicable law.

If the application or its services are directed at children, or are likely to be accessed by children, the Data Controller will apply the relevant requirements of UK data protection law, including applicable provisions of the UK GDPR, the Data Protection Act 2018 and the ICO's Children's Code (Age Appropriate Design Code), where applicable.

Where consent is relied upon as the legal basis for processing a child's personal data in connection with an information society service, specific rules concerning children under 13 may apply.

1. TECHNOLOGIES THAT STORE OR ACCESS INFORMATION ON THE USER'S DEVICE

Certain features of the application or related third-party services may use technologies that store information on the user's device or access information already stored on the device.

Where PECR applies, such technologies will be used in accordance with the applicable consent requirements and statutory exemptions.

Technologies that are strictly necessary to provide a service requested by the user may fall within an applicable exemption from the consent requirement where the relevant legal conditions are satisfied.

Technologies used for advertising, tracking or similar purposes will not be treated as strictly necessary merely because they contribute to financing or monetising the application.

1. CHANGES TO THIS PRIVACY POLICY

The Data Controller may periodically update this Privacy Policy to reflect changes to the application, third-party services, applicable law or data processing practices.

Where material changes are made, users may be notified through the application, the relevant website or by publication of an updated version of this Privacy Policy.

The current version of this Privacy Policy will be available at:

[PRIVACY POLICY URL]

1. CONTACT

For matters concerning personal data protection, privacy or the operation of the application, users may contact the Data Controller at:

support@sidekickaimanager.app

PerfectWiFi – Privacy Policy United Kingdom

Version: 1.0 Effective date: 9 August 2026