Last updated: March 2024

This privacy statement applies only to the “Do-fit” application services provided by Shenzhen Black White Grey Communication Technology Co., Ltd. (hereinafter referred to as “we” or “Black White Grey”) for you, including device binding, sports health data and other services.

This privacy statement will help you understand the following:

1. How we collect and use your personal information;
2. How we transfer and disclose your personal information;
3. How we collect and protect your personal information;
4. Permission Call Instructions
5. Third-party SDK terms and conditions
6. Your rights;
7. How do we handle children’s personal information;
8. Data storage location and duration;
9. Self-starting and associated starting;
   How this privacy statement is updated;
10. How to contact us.

We are deeply aware of the importance of personal information to you and will do our utmost to protect the security and reliability of your personal information. We are committed to maintaining your trust in us and abide by the following principles to protect your personal information: consistency of rights and responsibilities, clear purpose, choice and consent, minimum necessary, ensure security, subject participation, openness and transparency. At the same time, we promise to take corresponding security measures to protect your personal information in accordance with mature security standards in the industry. Please read and understand this privacy statement carefully before using our products (or services).

1. How do we collect and use your personal information

1.1 Personal information refers to various information recorded in electronic or other forms that can be used alone or in combination with other information to identify the identity of a specific natural person or reflect the activities of a specific natural person.

1.2
The “Do-fit” app is used to record and analyze user movement and health data. In order to provide sports and health services, it is necessary to collect and use your personal information. The personal information referred to in this statement includes device

information, personal data, sensor data, movement data, and health data. We will only collect and use your personal information for the following purposes stated in this statement:

- Binding of watch devices

To support the binding of your watch device and application, we may collect the identification information of your watch device, the identification information of your mobile device, the model number of your mobile device, the system version number, the Bluetooth information of your watch, and sensor data.

The purpose of collecting device MAC addresses is to enable Bluetooth connection binding between users and watch devices for data communication. The purpose of collecting software installation lists is to enable users to select target applications in an installation list for notification messages to be pushed to the watch side.

- Personal information

Including your height, weight, gender, age, and step length, this information can help calculate exercise data more accurately.

- Sports data

These include data such as device location, motion trajectory, motion type, motion duration, step count, distance, calories, and calculated analysis data, which are used to store and display for users.

- Health data

These data include sleep, heart rate, stress, blood oxygen, etc., which are used to store and display for users.

1.3 In order to protect the rights of black, white, and gray customers, we will conduct risk control based on the information collected above to prevent fraud and other illegal activities. If you do not provide such information, we may not be able to provide you with the full range of services described above.

2. How do we transfer and disclose your personal information publicly

2.1 Transfer

We will not transfer your personal information to any company, organization or individual, except in the following circumstances:

- Transfer with explicit consent: We will transfer your personal information to other parties after obtaining your explicit consent;
- When it comes to mergers, acquisitions, or bankruptcy liquidation, if personal information transfer is involved, we will require the new company or organization that holds your personal information to continue to be bound by this privacy statement, otherwise we will require the company or organization to seek your authorization and consent again.

2.2 Public disclosure

We will only publicly disclose your personal information in the following circumstances:

After obtaining your explicit consent;

- Disclosure based on law: We may publicly disclose your personal information under the mandatory requirements of laws, legal procedures, litigation, or government authorities.

3. How do we protect your personal information

3.1
We will use industry-standard security measures to protect the personal information you provide and prevent unauthorized access, disclosure, use, modification, damage, or loss of data. We will take all reasonable and feasible measures to ensure that irrelevant personal information is not collected. We will only retain your personal information for the period necessary to achieve the purposes described in this statement, unless an extended retention period is required or permitted by law.

3.2
The Internet environment is not 100% secure. We will try our best to ensure or guarantee the security of any information you send us. If our physical technology or management protective facilities are damaged, resulting in unauthorized access, public disclosure, tampering, or destruction of information, we will promptly inform you of the basic situation and possible impact of the security incident, the measures we have taken or will take to dispose of it, suggestions for you to independently prevent and reduce risks, and remedial measures for you in accordance with laws and regulations. We will promptly inform you of the relevant situation of the event through email, letter, phone, push notifications, and other means. If it is difficult to inform the personal information subject one by one, we will take reasonable and effective

measures to publish an announcement. At the same time, we will also proactively report the handling of personal information security incidents in accordance with regulatory requirements.

4. Do-fit permission call description

In addition, the following device permissions may be triggered when you use Do-fit. To help you better manage your information, we will inform you of the purpose of using the permission during the permission request process during product use, as well as the impact on your use of the service if you do not enable the permission. Please review carefully. Before using a specific feature, you can choose whether to authorize the following permissions. At the same time, you can change your authorization status at any time through the device permission settings page.

The following details the relevant functions and calling permissions for your reference:

(I) Android

4.1 Read and write external storage space: used to read pictures on the phone when the user sets the dial plate image; when the user shares pictures, it is used to save the pictures on the user's phone; when the user sets the avatar to "choose from the photo album", it is used to save the cropped picture on the user's phone.

4.2 Accessing the camera: Used for users to set their avatar and select the "Take Photo" option to save the photo on their phone; used for users to take photos (remote control) and save the photo on their phone.

4.3 Location permission: used to scan Bluetooth devices when users are binding wearable devices; when users turn on the motion function, it is used to help users record motion tracks; used to synchronize weather information displayed on wearable devices for users;

4.4 Read Contacts: used to synchronize contacts to the device when the user uses the "Sync Contacts" function; used to synchronize the incoming call number and contact name to the wearable device for display when the user uses the "Call Reminder" function;

4.5 Call records: used to synchronize the incoming call number and contact name to the wearable device for display when the user uses the "call reminder" function;

4.6 SMS permission: used to synchronize the sender's name/number and SMS content to the wearable device for display when the user uses the "SMS reminder" function;

4.7 Access notification permissions: Used by users to push messages to devices using the message push function (message types include but are not limited to WeChat, QQ, Facebook, Twitter, Line, WhatsApp).

4.8 Access to the list of installed applications: This is used for users to select applications to enable the message push function to push messages from the application to the watch device.

(II) iOS

4.1 Access to camera albums and microphones: Used by users to take photos (remote control photography) and save photos on their phones.

4.2 Location permission: When the user turns on the motion function, it is used to help the user record the motion track; it is used to synchronize the weather information displayed on the wearable device for the user;

4.3 Address book: used to synchronize contacts to the device when the user uses the “synchronize contacts” function; used to synchronize the incoming call number and contact name to the wearable device for display when the user uses the “call reminder” function;

5. Third-party SDK terms and conditions

Please note that when you use and access our services, you may also be subject to the terms and conditions and privacy policies of certain third parties such as app stores, map providers, mobile software platforms, social networking sites, and payment intermediaries. You acknowledge and agree that we are not responsible for the terms and conditions of these third parties or how they use your personal information. We may choose to link you to third-party products or services through advertising or other forms at our discretion. Please note that the third-party products and services you use are not developed or managed by the people or businesses we are affiliated with or control. We are not responsible for the actions, products, and services of these people or businesses, nor how they use the information you provide. Our providing links to them does not create a relationship of association or control between us and them. We may provide services of our partners at any time, such as quiz games, surveys, etc. Their services may require you to provide personal information to register or access. These services will indicate the identity of the partner when you need to disclose personal information. If you choose to disclose personal information, then this data may be provided directly or indirectly to third parties through us. You will accept their privacy policies and practices. We are not responsible for the privacy policies and practices of these third parties. Therefore, you should review their privacy policies and practices before disclosing personal information. Please note that in our services, some items may use third-party

services to compare and verify game identities, online shopping accounts, social accounts, network accounts, and other information. If you choose to participate in or use these services, certain personal user or account data and sensor data may be automatically transmitted to these third parties. You hereby agree that we will process, use, integrate, disclose, and retain this data in accordance with this policy.

For example, in the following circumstances, we may share your personal information with third-party service providers. Before using this feature, you confirm that you have carefully read the user agreement and relevant privacy policies of the third-party service.

5.1 Baidu positioning SDK: The map service of the application is provided by Baidu Map (SDK:com.baidu.mapapi). We will provide your GPS positioning information to such service providers through SDK related technologies, to provide you with map-based, motion-related positioning services. Baidu Map privacy policy: https://lbsyun.baidu.com/index.php?title=openprivacy

6. Your Rights

6.1 You can go to “My” > “About” > “Privacy Statement” > click “Disagree with this Privacy Statement” to revoke authorization.

6.2 If you have further requests or any questions, comments or suggestions regarding your data subject rights, you can contact us through the methods described in the “How to Contact Us” section of this statement and exercise your relevant rights.

6.3 To ensure security, you may need to provide a written request or otherwise prove your identity. We may first require you to verify your identity before processing your request. We will respond as soon as possible.

6.4
For your reasonable requests, we do not charge fees in principle, but for repeated requests that exceed reasonable limits, we will charge a certain amount of costs depending on the situation. For those unfounded and repetitive requests that require excessive technical means (such as the need to develop new systems or fundamentally change existing practices), pose risks to the legitimate rights and interests of others, or are very unrealistic, we may refuse them.

6.5 We will not be able to respond to your request in the following circumstances:

- In relation to fulfilling obligations under laws and regulations with personal information controllers;
- Directly related to national security and defense security;
- Directly related to public safety, public health, and major public interests;
- Directly related to criminal investigation, prosecution, trial, and execution of sentences;
- The personal information controller has sufficient evidence to indicate that the personal information subject has subjective malice or abuse of power;
- It is necessary to protect the vital legal rights and interests of the personal information subject or other individuals, such as their lives and property, but it is difficult to obtain their consent;
- Responding to the request of the personal information subject will cause serious damage to the legitimate rights and interests of the personal information subject or other individuals or organizations;
- Involving trade secrets.

7. How do we handle children's personal information

7.1 This application is only for adults. Children should not create their own personal information account without the consent of their parents or guardians. Parents and guardians should also take appropriate precautions to protect children, including supervising their use of this application.

7.2
Although the definition of children varies from place to place based on local laws and customs, we consider any person under the age of 14 to be a child. For cases where parents have consented to the collection of children's personal information, we will only use or disclose this information when permitted by law, with the explicit consent of the parent or guardian, or when necessary to protect the child.

8. Data storage location and duration

8.1 Data storage location

If you are a user in Chinese Mainland, the personal information we collect and generate under this service will be stored on the server located in Chinese Mainland; If you are a user in a country or region other than Chinese Mainland, your data will be stored on the server in Singapore.

8.2 Data storage period

We only retain your personal information for the time necessary to achieve our purpose, which is 1 year. After the expiration of the data retention period, if you no longer use our products, we will delete or anonymize your data within a reasonable period of time, unless otherwise required by law or regulation; if you are still using our products, we will automatically extend the retention period by 1 year to continue to provide more professional sports health services.

9. Self-starting and associated starting

9.1 This app needs to remain running in the background to ensure that the connected smart watch can receive real-time message reminders, phone reminders, etc. It is necessary to use self-starting capabilities, which will send broadcasts through the system at a certain frequency to wake up the app for self-starting or associated starting behavior. This is necessary to implement this feature and service.

10. How to update this privacy statement

10.1 Our privacy statement may change. Without your explicit consent, we will not reduce your rights under this privacy statement.

10.2 For major changes, we will also provide more prominent notifications. Major changes referred to in this statement include but are not limited to:

- Our service model has undergone greater changes. Such as the purpose of processing personal information, the type of personal information processed, and the use of personal information;
- We have undergone significant changes in ownership structure, organizational structure, etc. Such as changes in ownership caused by business adjustments, bankruptcy mergers, etc;
- The main object of personal information sharing, transfer, or public disclosure has changed;
- Significant changes have occurred in your rights and methods of exercising your rights in relation to personal information processing;
- When the responsible department, contact information, and complaint channel for handling personal information security changes;
- When the personal information security impact assessment report indicates high risks.

11. How to contact us

11.1 We have established a dedicated department for personal information protection (or personal information protection officer). If you have any questions, comments or suggestions about this privacy statement, please contact us at the following email address: suggest@blackwhitegreygroup.com, and we will respond as soon as possible.

11.2 If you are not satisfied with our response, especially when our personal information processing behavior harms your legitimate rights and interests, you can also resolve it through external channels such as filing a lawsuit with a competent people's court, complaining to industry self-regulatory associations or relevant government regulatory agencies. You can also ask us for information about possible applicable complaint channels.