Data Privacy Policy

Version No. V1.0.9

Last updated: 01 February 2024

App: POLICE FOT

Developer:

We take the protection of your personal data very seriously and want you to feel secure when using our app and products. The protection of your privacy when processing personal data is an important concern for us that we also consider in all our business processes.

Personal data are collected, processed, and used exclusively in accordance with legal regulations and in good faith. As far as possible, we design our business processes in such a way that the data protection requirements are already considered during the development of the products and service offers and to the extent possible, personal data is pseudonymized.

Information we collect

As part of our business relationships, we process personal data that we have received directly from you. In addition, we process personal data which we legitimately obtain from publicly accessible sources, or which is legitimately transmitted to us by other third parties, insofar as this data is necessary for the provision of relevant services, we provide to you and/or within the scope of the Purposes as set forth below.

Purposes of processing ("Purposes") and legal basis

Your personal data will be processed in accordance with the provisions of the GDPR and for the following purposes.

For the fulfillment of contractual obligations (Art. 6 Para. 1 b GDPR): The processing of personal data takes place in the context of trade with products and services in the field of consumer electronics. The Purposes of data processing depend primarily on the specific product and its software applications. Further details on this data processing purpose can be found in the accompanying operating instructions, manuals and other terms and conditions at the purchase of such specific products.

Within the framework of the balancing of interests (Art. 6 para. 1 f GDPR): If necessary, we process your data beyond the actual performance of the contract to protect the legitimate interests of us. for the purpose of the assertion of legal claims and defense in legal disputes; the guarantee of IT security and the maintenance of our IT infrastructure and operation; the prevention and clarification of criminal offenses; and for business management purposes and the development of services and products.

Based on your consent (Art. 6 Par. 1 a GDPR): If we have your consent to the processing of personal data for specific purposes (e.g., forwarding of data within the Group or evaluation of data for marketing purposes), the legality of such processing is given based on your consent. The given consent can be revoked at any time at our App (Settings Withdraw Consent). The revocation of the consent does not affect the legality of the data processed until the revocation.

Due to legal requirements (Art. 6 para. 1 c GDPR) or in the public interest (Art. 6 para. 1 e GDPR): This includes, for example, identity and age checks or the fulfillment of tax control and reporting obligations.

Special data protection at our Fitness tracker: We use your data to make the use of the Fitness tracker as pleasant as possible for you and so that you can benefit optimally from your fitness program. At the same time, this information will improve our Service. The application stores and processes the following data: Username, Gender, Birthday, Weight, Height, Steps, sleeping hours, heart rates (if available), distances, calorie consumption, goals, successes, and challenges. Your data will only be stored locally on your smartphone or device. To ensure the compatibility of your Smart Watch with your smartphone or device, our Smart Watch/ application accesses the following functions of your phone:

Android

1. Read caller list

2. Taking picture and videos

3. Reading contacts

4. Receive SMS

5. Read SMS or MMS

6. Read the contents of your shared memory

7. Changing or deleting the contents of your shared memory

8. Only access the exact location when running in the foreground

9. Access the approximate location (network-based) only when running in the foreground.

10. Accept calls

11. Retrieve phone status and identity

12. Retrieve network connections

13. Battery performance optimisations

14. Perform linking with Bluetooth devices

15. Execute foreground service

16. Access Bluetooth settings

17. Control vibration alarm

18. Access to all networks

19. Deactivate idle state

20. Play install Referrer API

iOS

1. Location

2. Photos

3. Bluetooth

4. Camera

5. Siri & search

6. Messages

7. Background update

8. Mobile data

App permissions: To provide you with the functionalities of the app, the app must be able to access various functions and data of your mobile device. To do this, it is technically imperative that you grant the app selected access authorizations. Otherwise, the app cannot be used for technical reasons. Before using the app for the first time, we will explicitly inform you of the requested access rights. Usually the authorizations are as follows:

Location: This permission is required to determine your current location for location-based services. This permission allows your phone to access your GPS data, WLAN identifiers and/or Bluetooth, depending on which of them you have enabled, to locate your location.

Push notifications: Push notifications are messages (e.g.: WhatsApp) that are sent from the app to your device and are prioritized there. This app uses push notifications on delivery, provided the user has consented during the installation of the app or the first use. End user has to accept the enable notifications for the first-time installation. Also, the reception of push notifications can be deactivated at any time in the settings of the app.

Access smartphone contacts: This permission is required to show the caller's name when the user received a call notification.

User behavior: Within the framework of legal regulations, we, or companies commissioned by us, create user profiles, enter a name, or insert an Avatar in our App. Users can click "skip" to not provide this information. The profile data is not linked to any further information about the user. Device information: In addition to protocol data, we may also collect information about the device on which the app is used. These include device type, operating system used, device settings, unique device identifiers and crash data. Whether some or all this information is collected depends on the type of device used and its settings. This allows error messages and system crashes to be analyzed to improve future operation. You can find out from
https://www.gstatic.com/policies/privacy/pdf/20210701/7yn50xee/google_privacy_policy_en.pdf how the information is processed and protected.

We are distributing our App via Apple App Store and Google Play Store. We have also incorporated Google Maps (for Android devices), Firebase Crashlytics, and Google Analytics in our App. GPS related sport activities and Google Maps require Location Permissions. Firebase Crashlytics and Google Analytics collect crash data that are not linked to any of your identity. The purpose of use Google Maps is to provide the latitude and longitude information from our GPS Smartwatch and to our app, then our App invoke Google Map to display user activity trajectory on the app which is a major function of our GPS Smartwatch. Google Analytics helps to measure and provides insight on our Watch App usage and user engagement. Analytics integrates across Firebase features and provides unlimited reporting for up to 500 distinct events that you can define using the Firebase SDK. Analytics reports help you understand users' behavior, which enables them to optimize app performance. The purpose of using Firebase Crashlytics and Google Analytics to collect crash data is to help to track, prioritize, and fix stability issues that erode our app quality. Crashlytics saves our troubleshooting time by intelligently grouping crashes and highlighting the circumstances that led up to them. Find out if a particular crash is impacting a lot of users.

Get alerts when an issue suddenly increases in severity. Figure out which lines of code are causing crashes.

As a result, usage of our apps is also subject to the following privacy policies:

• Apple App Store: https://www.apple.com/legal/privacy

• Google Play Store: https://policies.google.com/privacy

• Google Maps: https://policies.google.com/privacy

• Apple Maps: https://www.apple.com/legal/privacy/

• Google Crashlytics & Google Firebase Analytics: https://policies.google.com/privacy

• Open Weather: https://openweather.co.uk/privacy-policy

• Apple Health: https://www.apple.com/legal/privacy/en-ww/

• Google Fit: https://developers.google.com/fit/policy, https://policies.google.com/privacy

• Strava: https://www.strava.com/legal/privacy#full_policy

• Facebook：https://www.facebook.com/about/privacy

• Instagram：https://help.instagram.com/519522125107875

• Skype： https://support.skype.com/en/skype/all/privacy-security/

• Mailo: https://www.mailo.com/mailo/en/privacy-rules.php

Social Media: If you connect to this app via third party social media sites (such as Facebook, Twitter, Instagram or Google+), you may be subject to the data policy of such third-party social media sites. We do not have access to any of your personal data stored on such third-party social media sites.

The purpose of using weather service is that Weather is a major function of our Smartwatch. We make use of the device longitude and latitude information to query weather data for that location. The location information being collected is not linked to your identity and will not be stored or used for any other purposes. The usage of weather service and its storage duration of data are subject to their privacy policy: https://openweather.co.uk/privacy-policy

Data transfer to third countries or international organization

Our App is using 3rd party European based servers to provide firmware update service. Data is transmitted to offices in countries inside the European Union. No data will be transferred to third countries or international organizations outside the European Union According to Article 45 GDPR, transmission is permissible if the European Commission has decided that an adequate level of protection exists in a third country. In the absence of such a decision, we or the Service Provider may only transfer personal data to a third country or to an international organization if appropriate safeguards are provided (e.g., standard data protection clauses adopted by the Commission or the Supervisory Authority in a particular procedure) and enforceable rights and effective remedies are available. We have agreed contracts with these service providers for so-called order processing, which stipulate that the principles of data protection are always concluded with their contractual partners in compliance with the European data protection level.

Personal data and Measurement data recorded & processed.

Username, Gender, Birthday, Weight, Height, Steps, sleeping hours, Heart rate (if available), Running distance, Calorie consumption, Goals, Successes and Challenges.

Data Safety

As part of the App functionality, this App may collect the following data and upload it to your smartwatch as per your instructions and permissions. The collected data is processed ephemerally and will not be shared with third parties.

1. Contacts

2. Image

3. Media

4. Notifications

5. SMS

Data Protection and Limited Use Disclosure

All data transfer and storage are encrypted to protect this App against unauthorized or unlawful access, destruction, loss, alteration, or disclosure.

Health Connect: The use of information received from Health Connect will adhere to the Health Connect Permissions policy, including the Limited Use requirements.
https://support.google.com/googleplay/android-developer/answer/9888170?sjid=13972659535113455728-AP#ahp

Storage Period

Your data is only stored on your smartphone or device. Once the App is uninstalled, all personal data will be removed from your smartphone or device and none of the data will be retained. The retention period of data transmitted to third-party providers are subject to the data policy of such third-party social media sites. We will not actively transfer your data to any third party. The data that has been successfully transferred to a third party (e.g.: Apple Health, Google Fit or Strava (if available)) with your permission will follow the third-party platform and privacy policy. You can turn off third party authorization the setting at any time and data will no longer be transmitted. For firmware update, the data stored in European servers will be stored during your use of our Watch App. You can contact us to delete. Once you make a deletion request, we will delete or anonymize your information as soon as possible, and no later than 90 days from the date of your deletion request. The data will store around six months until a further new update is available if a deletion request is not made.

Affected rights: Any person concerned by the processing of personal data has the right to:

1. Information (Art. 15 GDPR),

2. Corrigendum (Art. 16 GDPR),

3. Cancellation (Art. 17 GDPR),

4. Restriction on processing (Art. 18 GDPR),

5. Data transferability (Art. 20 GDPR)

6. Opposition (Art. 21 GDPR).

There is a right of appeal to a competent data protection supervisory authority (Art. 77 GDPR). You also have the right to lodge a complaint with the responsible data protection supervisory authority at any time. You can contact the responsible data protection supervisory authority located in your country or state. You can revoke your consent to the processing of personal data at any time. You can uninstall our App anytime if you would like to revoke this consent. Please note that the revocation will only take effect in the future. Processing that took place before the revocation is not affected by this.

Automated decision making

In principle, we do not use fully automated decision making according to Art. 22 GDPR for the establishment and implementation of the business relationship. Should we use these procedures in individual cases, we will inform you separately, insofar as this is required by law.

Information about your right of objection according to Art. 21 Basic Data Protection Ordinance (GDPR)

Right of objection in individual cases You have the right to object at any time for reasons arising from your situation to the processing of personal data concerning you, which is based on Art. 6 para. 1 e GDPR (data processing in the public interest); this also applies to profiling based on this provision within the meaning of Art. 4 no. 4 GDPR. If you object, we will no longer process your personal data, unless we can prove compelling reasons worthy of protection for the processing, which outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims. Our app cannot be used if you revoke consent.

Withdraw your consent.

If you have given consent under this privacy policy to the processing of your data by our App. You can withdraw consent from our App (Settings Withdraw Consent-Press "OK") and none of the data will be retained You have the right to object at any time by writing to the following points of contact:

Notifications from the APP.

By accepting this privacy policy, you accept push notifications from the APP which will include information about upgrades and marketing. To opt out of receiving these notifications, you can deny permission within your phone's settings. By accepting this privacy policy, you accept in-app notifications from the APP which will include information about upgrades and marketing. To opt out of receiving these notifications, you can deny permission within the APP's settings.

Point of contact: If you have further questions regarding the processing of your data or wish to exercise any of your rights under the GDPR or pursuant to this policy, you can contact our data protection Controller at liping@zhilianshengya.net If you are based in Europe, you may also direct your inquiry to the data protection officer of our representative in Europe at liping@zhilianshengya.net Controller Details:

Shenzhen Zhilianshengya Technology Co.,Ltd ,
Address: 5F, Building B, Huawan Industrial, Xixiang Street, Bao'an District, Shenzhen

Email: liping@zhilianshengya.net
European Representative: Shenzhen Zhilianshengya Technology Co.,Ltd ,

Address: 5F, Building B, Huawan Industrial, Xixiang Street, Bao'an District, Shenzhen

Email: liping@zhilianshengya.net

Amendments to the Privacy Policy

We reserve the right to amend the Privacy Policy all times. Modifications will be posted here, on our website and we suggest that you review the Privacy Policy from time to time.

01 February 2024