HSBC Private Banking Switzerland - App Privacy Notice

HSBC Private Bank (Suisse) SA ('HSBC') collects, uses and shares information about you so that it can provide you with a bank account and related services. This App Privacy Notice explains how HSBC collects, uses and shares your information when you use this app, including information about the device that the app is installed on e.g. your mobile phone or tablet. You can find full information in our main privacy notice
https://www.privatebanking.hsbc.com/privacy-notice/. This app is provided by HSBC PB Services (Suisse) SA (located in Geneva, Switzerland) for and on behalf of HSBC, and all products and services accessed via this app are provided by HSBC.

For further information on anything related to this App Privacy Notice, or to contact our Data Protection Officer ("DPO"), write to quai des Bergues 9-17, 1201 Geneva, Switzerland , marking your letter "For the attention of DPO". To exercise your privacy rights, you can write to quai des Bergues 9-17, 1201 Geneva, Switzerland and marking the letter for the attention of "Rights of Individuals Fulfilment (ROIF)". Alternatively, you can contact us via the HSBC Switzerland Mobile Banking App where you can chat to us 24/7, via telephone banking or in branch.

We use a range of measures to keep your information safe and secure which may include encryption and other forms of security. We require our staff and any third parties who carry out any work on our behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate measures for the use and transfer of information.

We'll keep your information in line with our data retention policy. For example, we'll normally keep your main banking information for a period of ten years from when our relationship with you ends. This allows us to comply with legal and regulatory requirements or use it where we need to for our legitimate purposes such as managing your account and dealing with any disputes or concerns that may arise. We may need to keep your information for longer where we need the information to comply with regulatory or legal requirements, help detect or prevent fraud and financial crime, answer requests from regulators etc. If we don't need to keep information for this length of time, we may destroy, delete or anonymise it sooner.

You acknowledge and accept that, by downloading the HSBC Private Banking Switzerland App and by using such App, the operator of the app store (for example Google or Apple) may infer the existence of a banking relationship between HSBC and you.

The tables below explains what information HSBC collects from your device, how it uses it, and whether it shares it.

In some cases, e.g. when accessing the contacts stored on your device, or photos that you take with your device, HSBC will first ask your permission. HSBC may share your information with other HSBC group companies and any sub-contractors, agents or service providers who work for us or other HSBC group companies (including their employees, sub-contractors, service providers, directors and officers) to provide you

with products or services that you ask for (such as bank accounts and payments) and as explained in our main privacy notice - this type of data sharing is not included in the tables.

Android permissions

Permission	Used for
Internet connection	Allows applications to connect to the internet.
Internet connection check	This allows us to check if you have a working internet connection.
Device state	Allows us to know if you are on a call while using the app. This helps us to detect and prevent fraud.
Device storage check	This allows the app to save files onto your device's external storage.
Device storage	This allows the app to save and send files from your device's external storage.
WiFi connection	This allows us check if you have a working internet connection.
Communication	Allows Samsung devices to support Firebase Cloud Messaging & Apple Push Notification Service (see "Cookies" section).
Communication	Migrated from Google FCM. Create an instant-enabled app bundle	Android Developers
Prevent phone from sleeping	Required by older versions of Google Play services to create Firebase Instance ID tokens. These tokens allow us to send notifications to customers.
Biometric recognition	Allows an app to use biometric recognition for your authentication. If you do so, we rely on your device's technology to authenticate you and we do not collect or store your underlying biometric data.
Notification	Allows an app to popup notifications
Google firebase Advertising ID	Allows an app to get the Google firebase Advertising ID, Google push feature will depends on this.

Apple permissions

Permission	Usage Description
Camera access	Allows our app to use facial recognition for your authentication.

Facial recognition	Allows our app to use facial recognition for your authentication. If you do so, we rely on your device's technology to authenticate you and we do not collect or store your underlying biometric data.
Location	Allows our app to access your location to help us detect and prevent fraud.

Cookies:
Our app includes tools that collect information about your device and the way you use it online to:

- track app performance so that it can keep running smoothly.
- recognise your approximate location.
- detect and prevent malware and fraud, by collecting information about potential risks on your device, for example if it's jailbroken or rooted, or if there are untrusted software keyboards or screen readers installed.
- track your activity within the app to support future enhancements.
- secure your login and authentication.
- track the performance and usage of videos.