TRUSTED PRIVACY
EU data protection
ePrivacyseal

CERTIFICATE

no. 445/23

ePrivacyseal GmbH
Große Bleichen 21, 20354 Hamburg, Germany

hereby certifies* that

as determined in the certification decision of 30 May 2023

Vivo Tech GmbH
Speditionstr. 21, 40211 Düsseldorf, Germany
as a controller in the sense of art. 4(7) GDPR

operates its product or service
„iManager“
version 3.0.6.1 as of 10 April 2023
as defined in annex 1 and to the exclusion of the processing activities in annex 2 to this certificate

in conformity with the criteria catalogue for the “ePrivacyseal EU” (version 3.0 of May 2022)
of ePrivacyseal GmbH.

final audit day: 30/05/2023
next planned monitoring by 31/03/2026
period of validity: 01/04/2023 – 31/03/2026

*ePrivacyseal GmbH is not an accredited certification body within the meaning of art. 42(5) GDPR.

Annex 1 to certificate no. 445/23

Definition of processing activities

The target of evaluation "iManager"-solution implemented on Vivo devices is a built-in resource manager, acting like a phone cleaner, data monitor, application and phone manager. It scans the pictures, videos, audio files, trash, and other data of users, shows them to users and provides the deletion option; scans the app installed on the user's mobile phone, acquires for how long the apps have been unused and provides the uninstallation option. The app has the following functions:

1. **Automatic cleanup** (in case of insufficient storage space).
   This includes emptying the recycle bin, the items that were recently deleted from the albums, and the data that remained on the smartphone after uninstalling apps. All options can be enabled or disabled.

2. **A threat detection**
   This is implemented by AVAST's antivirus engine. A detection reminder (30, 60 or 90 days) and an update reminder (30, 60 or 90 days) can be set. The virus protection can be updated to the latest version via WLAN without using mobile data. When performing a security scan over Wi-Fi, the system detects apps on the smartphone and scans them for viruses or risks. To get more accurate search results, this is done via the cloud. There is a setting for automatic update via Wi-Fi and/or mobile network and in the area of automatic detection via online cloud scan also via Wi-Fi and/or mobile network. Auto-detection can be done every 7, 15 or 30 days, with scanning done in the background at night. In addition, there is a whitelist for risky apps.

3. **Other security features**
   a) App security detection
      Apps downloaded and installed from the vivo appstore or other sources are automatically detected and checked for security risks.
   b) Screen capture protection
      If a password is entered on login or payment pages, malicious apps are prevented from taking screenshots or recording the screen to protect the password and prevent disclosure.

Furthermore, iManager provides information and setting options about apps and notifications. Also, the usage time of the device can be displayed and listed in detail by individual apps. There is a function to "clone" apps (like Facebook or Instagram) to exclude them from accessing personal data. In addition, standard apps can be configured and permissions can be set for individual apps via the permission manager. In this way, access to data can also be set. This is necessary and useful for the iManager itself, for example, and for the integrated "Album" app.

Downloading the app is not necessary, as it is integrated. Data does not flow out of the app, except when sending data to AVAST for malware scanning.

Annex 2 to certificate no. 445/23

Excluded processing activities

This evaluation refers only to the above mentioned product and therefore only to the processes in which Vivo Tech GmbH and its customers are involved.

The following functions are not within the scope of the evaluation:

1. The website of vivo
2. Any other registration possibilty of the user on the phone
3. Any other app installed on the app

*ePrivacyseal GmbH is not an accredited certification body within the meaning of art. 42(5) GDPR.