Privacy Policy baramundi Mobile Devices (bMD)

baramundi Mobile Devices, the solution for managing mobile devices, has been designed and developed with the utmost care in compliance with German data privacy regulations. Our solution supports administrators in securely integrating mobile devices into their company's internal IT infrastructure. The solution is concerned with managing devices, not the content of applications.

For the baramundi Mobile Devices (bMD) module, we warrant that the design of the baramundi Management Suite combined with the locally installed baramundi Agent app precludes the following activities:

- bMD does not read any contact data (names, telephone numbers, etc.) from the address book
- bMD cannot record SMS text messages (neither connection lists nor content)
- bMD does not enable access to the content of e-mail boxes.
- bMD does not record any call lists
- bMD does not enable access to the content of other communications apps such as WhatsApp
- bMD cannot intercept phone calls
- bMD does not have access to the microphone in order to tap the surroundings
- bMD does not enable access to media files (images, videos, etc.)
- bMD does not store location information locally, nor is it transmitted to the server. The only exception is devices in "lost" mode.

The following types of access to smartphone hardware are used to only a very limited extent:

- bMD accesses the camera only in order to read the QR code as part of the registration process
- bMD uses location services to locate a device in "lost" mode. If lost mode is activated, the user receives a corresponding message.
- bMD requires access to the location services under Android Enterprise in the "Fully Managed" and "Dedicated Device" profile to inventory the Wifi networks stored on the device.
- bMD requires access to the location services under Android Enterprise in the "Work Profile" to inventory the Wifi networks stored in the profile. Wifi networks manually created on the device by the user are not transferred to the server.

bMD is in fact designed to perform the following typical management activities (this list is not exhaustive):

- Creating an inventory of the installed apps
- Detecting manipulations of firmware (Jailbreak*, Root)
- Configuring security features and restrictions
- Remote removal of the device/installed apps

*) To optimize manipulation detection for iOS, we recommend using baramundi’s push service infrastructure. Here, the baramundi management server transmits the following data to a central baramundi service:

- A clear, anonymous identifier for the bMS installation
- The push token generated by Apple for the device
- The iOS version of the device
- The version of the bMD Agent app

This function can be activated in the bMD configuration and is disabled by default.

A more detailed description of bMD’s features can, for example, be found in the release notes.