CylancePROTECT Mobile for UEM Privacy Data Sheet

About this Data Sheet

This Privacy Data Sheet describes the processing of personal data by the Mobile Threat Defense features of BlackBerry© UEM and BlackBerry Dynamics™. It provides details about how and why customer data is processed and is provided for informational purposes only. The information provided is current as of the "last updated" date of this document. For an up-to-date list of Subprocessors, please see BlackBerry's [Subprocessor listing](#).

This Privacy Data Sheet is supplementary to the UEM On-Premises, UEM Cloud and BlackBerry Dynamics Privacy Data Sheets.

BlackBerry Privacy Office

BlackBerry has a dedicated Privacy Office that, in partnership with BlackBerry Information Security, assesses our technical and administrative security controls to ensure compliance with international legislative requirements governing privacy matters.

BlackBerry complies with data protection and privacy laws concerning the collection, use, storage, transfer, and disclosure of personal data, including the EU General Data Protection Regulation.

Our commitment to customer privacy is detailed at www.blackberry.com/privacy.

Overview

CylancePROTECT® Mobile for UEM is a Mobile Threat Defense solution that augments the security capabilities provided by BlackBerry UEM. It prevents, detects, and remediates advanced malicious threats by identifying malware, while using BlackBerry UEM for device management, and BlackBerry Dynamics™ apps to enforce your security policies to get in front of malicious cyberattacks.

CylancePROTECT Mobile for UEM scans devices for vulnerabilities, malicious or sideloaded apps, identifies insecure networks and device settings that pose a security risk to provide an overall security assessment. It analyzes URLs in real-time to identify potentially unsafe sites accessed by BlackBerry Dynamics apps and in text messages when granted permissions on the device.

Information about the data collected by BlackBerry UEM and BlackBerry Dynamics apps can be found on the [Additional Privacy Resources](#) on BlackBerry.com.

Privacy Enhancing Technologies

BlackBerry uses industry standard encryption protocols to protect data during transmission and at rest. Data is stored on encrypted disks with 256-bit AES encryption.

Personal Data Processed

The following data elements are collected and processed by BlackBerry and could be considered personal data depending on your deployment. This data is collected in addition to the data collected by your UEM implementation.

Personal Data Processed	Purpose for Processing	Recipients
Mobile app data: Android APK Names, APK Developer signature, APK Binary Hash, APK Version, APK Package Name, APK Install source	• Detection of malicious or suspicious applications	• Customer Administrators • BlackBerry Service Management*
Mobile app data: iOS iOS Developer, iOS signer cert hash	• Detection of malicious or suspicious applications	• Customer Administrators • BlackBerry Service Management*

* All access by BlackBerry Service Management is incidental and not required in the normal course of providing the service. Access is restricted only to BlackBerry employees that are responsible for managing and monitoring this service.

Data Sharing or Forward Processing

BlackBerry uses the identified information to facilitate the performance of the End User License Agreement under which BlackBerry's services and products are offered. This data is only shared with necessary third-party services that are required to provide the services.

BlackBerry does not sell, lease, or otherwise distribute this information beyond what is disclosed in this data sheet.

Cross-Border Data Transfers

BlackBerry Limited is a Canadian corporation and primarily relies upon the European Commission's adequacy decision for data transfers from the EU/EEA, as well as to its UK subsidiary, BlackBerry UK Limited. For transfers to BlackBerry's U.S. subsidiary, BlackBerry Corporation, it relies upon an Intracompany Agreement that incorporates the 2021 EU Standard Contractual Clauses (SCCs), the UK SCC Addendum, and the Swiss Rider. In addition, BlackBerry offers customers a Data Processing Addendum that incorporates the 2021 EU SCCs, the UK SCC Addendum, and the Swiss Rider. If BlackBerry transfers personal data to a sub-processor, we ensure that: (i) the personal data is transferred to countries recognized as offering an adequate level of protection; or (ii) the transfer is made pursuant to appropriate safeguards, such as a Data Processing Addendum that incorporates the 2021 EU SCCs, the UK SCC Addendum, and the Swiss Rider.

BlackBerry is a global organization with Customer Support, Threat Research and Data Science personnel located in Canada, EU, India, Japan, Singapore, UK, and the U.S. BlackBerry utilizes follow-the-sun scheduling for Customer Support and as a result, support during normal business hours may be provided in-region, however urgent issues will be addressed by available global resources.

CylancePROTECT Mobile for UEM relies upon a customer's UEM established instance, which is where personal data used to manage the service is stored.

Information about detected device vulnerabilities, potentially malicious mobile apps and hyperlinks are stored in in the United States.

CylancePROTECT Mobile for UEM uses the following Subprocessors:

Subprocessor	Personal Data Processed	Location
Arctic Wolf Networks Malware analysis service provider	Mobile app data, SMS message data and browsing data	North America (United States)

Information about Subprocessors engaged by BlackBerry to support the delivery of BlackBerry UEM and BlackBerry Dynamics apps, along with other BlackBerry solutions, is available on BlackBerry's Subprocessor listing.

Data Retention

Personal Data Processed	Data Retention Period
Mobile app data: Android & iOS	Data is removed two months after the end of the contract.
Potentially malicious mobile apps	Data is de-identified and retained indefinitely.

Legal Notice