BlackBerry® Gateway Product Privacy Notice

About this Notice

This Product Privacy Notice is provided to offer transparency with regards to BlackBerry's data collection and processing activities. This document provides details about a specific BlackBerry Solution that collects personal data and provides key details on how and why customer data is processed.

BlackBerry Privacy Office

BlackBerry has a dedicated Privacy Office that, in partnership with the Cyber Security & Risk team, 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

BlackBerry Gateway is a network Security-as-a-Service designed to provide a best-in-class secure access service edge framework combining network security functions, such as Zero Trust network access and Secure Web Gateway, that gives users access to private and SaaS apps while protecting an enterprise network from threats. BlackBerry Gateway answers the need for a secure, trusted, and lightweight solution by providing network Security-as-a-Service as part of the BlackBerry Spark suite. It uses a lightweight app installed on users' devices, the established and trusted BlackBerry Infrastructure, and the AI/ML tools from BlackBerry Persona to secure connections from devices to cloud services and other web sites.

Privacy Enhancing Technologies

The BlackBerry Gateway app provides an additional layer of network protection by establishing a secure tunnel using the BlackBerry Infrastructure. BlackBerry Gateway has no visibility into network traffic and does not decrypt customers' traffic.

The BlackBerry Gateway AI and ML engine continuously manages a list of unsafe Internet destinations to prevent endpoints from accessing destinations that may threaten your devices, network, and information assets.

Personal Data Processed

The following personal data elements are collected and processed by BlackBerry on behalf of its customers.

Personal Data Processed	Purpose for Processing	Recipients
End user contact information User unique identifier, email, first name, last name	• Provide customer's authorized administrators with ability to configure capability and provide visibility into user's network activity.	• Customer Administrators • BlackBerry Product Support • BlackBerry UES and Common Service Management
Device information Hostname, OS vendor/version/build, last connected date/time	• Provide customer's authorized administrators with visibility into user's network activity and configure risk mitigation policies.	• Customer Administrators • BlackBerry Product Support • BlackBerry UES and Common Service management
Endpoint network activity DNS activity, destination IP address, destination port, TLS certificates, categories of network resources accessed, data transferred, date/time.	• Provide customer's authorized administrators with visibility into user's network activity and configure risk mitigation policies.	• Customer Administrators • BlackBerry Product Support • BlackBerry Gateway Service Management • BlackBerry Persona Service Management
Alerts and events Risk calculation, risk type, status, user's name, device name, network destination, action taken, data transferred, detection time and response actions.	• Provide customer's authorized administrators visibility to user's network activity that may present a risk to their organization and personnel.	• Customer Administrators • BlackBerry Persona Service Management • BlackBerry Product Support
Diagnostic information Information about problem, user provided email address for follow up (if provided), device details, user unique identifier, device unique identifier, data/time of event.	• Support problem reporting and issue resolution.	• BlackBerry Product Support • BlackBerry Engineering Team
Customer administrative login Login activity from administrators or operator of customers tenant, which includes date/time, user unique identifier, status, and account name.	• Audit authentication activity and perform risk management.	• Customer Administrators • BlackBerry Product Support

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 fulfill the intended purpose of this services.

BlackBerry will not sell, lease, or otherwise distribute this information beyond what is disclosed below.

Cross-Border Data Transfers

BlackBerry Gateway customers select the geographic location of their tenant, which is where personal data used to manage their service, along with data collected from endpoints is stored. Data is not transferred from the customers chosen tenant location to any other geographic region without the customers prior instruction or approval.

Customer Tenant Geography	Location	Sub-Processor
Asia Pacific	Australia, Sydney	Amazon Web Services
	Japan, Tokyo	
Europe	Germany, Frankfurt am Main	
South America	Brazil, Sao Paulo	
United States	United States, Northern Virginia	

Data Retention

Personal Data Processed	Data Retention Period
End user contact information	Data is stored for the duration of the MSA Agreement.
Device information	Data is retained for as long as a registered device is active.
Endpoint network activity	Data is retained for 30 days.
Alerts and events	Data is retained for 30 days.
Diagnostic information	Data is retained for 5 years.
Customer administrative login	Data is stored for the duration of the MSA Agreement.

Legal Notice