Privacy Policy

Use of baramundi Proactive Hub

Updated September 9, 2026

1. **Data Controller:**

The data controller pursuant to Art. 4(7) of the GDPR is baramundi software GmbH, Forschungsallee 3, 86159 Augsburg, Phone: +49 821 567 08 -0, Email: info(at)baramundi.com.

2. **Data Protection Officer**

You can contact the Data Protection Officer at privacy@baramundi.com.

3. **User account**

To use baramundi Proactive Hub, a user account with the following mandatory personal information is required:

- Email address
- Username
- Password

This data is required for user login to baramundi Proactive Hub.

The legal basis for the data processing required to fulfill the contract for the use of baramundi Proactive Hub is Article 6(1)(b) GDPR. The provision of your data is contractually agreed upon. Failure to provide this data would result in your inability to use baramundi Proactive Hub.

User data will be deleted immediately upon termination of the contract or upon request to delete your user account. Please contact support at proactive@baramundi.com

4. **Service Providers and Server Location**

We use cloud service providers whose data centers are located exclusively in the EU (Western Europe) or the USA (US East) for US environments.

5. **Cookies**

To enable secure login to baramundi Proactive Hub, we use technically necessary cookies. The providers of these cookies are baramundi software GmbH and Microsoft Corporation as the operator of Azure AD B2C. The legal basis for processing is our legitimate interest in secure login pursuant to Art. 6(1)(f) GDPR.

6. **Log Files**

Our cloud services log error messages. The following personal data is stored in the log files:

- User ID and email address of the application user
- IP address
- Device names
- Date and time of the request and of the application user's login and logout processes
- Time zone difference from Greenwich Mean Time (GMT)
- Address of the requested page
- HTTP status code
- Language, type, and version of the browser software
- Operating system of the application user

This data is necessary to analyze application errors as part of customer service and enables us to ensure the secure and trouble-free operation of the service. The legal basis for this is Art. 6(1)(f) GDPR.
Our legitimate interest arises from our role as the responsible operator of baramundi Proactive Hub.

We generate anonymized data from the log files to analyze and regularly improve the use of our baramundi Proactive Hub application. The statistics obtained allow us to improve our offering and make it more interesting for you as a user. The legal basis for this is Article 6(1)(f) GDPR. Our legitimate interest arises from our role as the responsible operator of baramundi Proactive Hub.

The log files are automatically deleted after 90 days.

7. Use of the baramundi Proactive Connect Wave browser extension

When using the baramundi Proactive Connect Wave browser extension, we collect and store interface-specific log data, such as search queries and technical logs. The log data is necessary for the operation, security, and traceability of the systems.
These log files are automatically deleted after 90 days.
Our legal basis is Article 6(1)(f) GDPR. Our legitimate interests lie in ensuring IT security, analyzing errors, and ensuring the stable and trouble-free operation of the systems.

8. Your Data Protection Rights

As a data subject, you have the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to object to processing, and the right to data portability.
To exercise your rights, please contact privacy@baramundi.com.

In addition, you have the right to lodge a complaint with a data protection supervisory authority. The data protection supervisory authority responsible for us is the Bavarian State Office for Data Protection Supervision (BayLDA) in Ansbach.

9. Information on data processing in connection with the use of the baramundi Proactive Connect Wave browser extension

To the extent that personal data is processed in connection with the use of the baramundi Proactive Connect Wave browser extension on behalf of our customers, such processing is carried out by baramundi software GmbH as a processor within the meaning of Article 28 GDPR.
Responsibility for this data processing, particularly with regard to the purposes of processing, the legal bases, and the fulfillment of data protection information obligations, lies with the respective customer as the data controller.
To ensure transparency, we describe below the categories of personal data that may be processed by us as a data processor in connection with the use of the browser extension, as well as the respective processing purposes and retention periods.

Data Category	**Description and Purpose of Processing**	**Retention Period**
Highlighted text	Text content highlighted by the user may be transmitted to the API during an active search query to identify relevant identifiers and perform search queries.	No local storage; up to 90 days on the server (in the logs)
Active page URL	The currently open page URL is read to display the referring domain and other contextual information within the extension.	No storage
DOM element information	To provide context functions, information about page elements is read when using the context menu, e.g., element type, CSS classes, IDs, or text content.	No storage
Authentication tokens	For authentication and authorization with backend services, access, ID, and refresh tokens are processed for login and authentication and stored locally in the browser.	Until logout, deletion of browser data, or uninstallation

Data Category	Description and Purpose of Processing	Retention Period
Email address	To display user information within the extension, the email address of the logged-in user is read from the ID token, stored locally in the browser, and displayed within the extension.	Until logout or deletion
User settings	To personalize the user interface, individual settings—such as region or the visibility of individual widgets—are stored locally in the browser.	Until changed or uninstalled
Session data (endpoints)	To enable navigation within the extension, information about recently visited endpoints is temporarily stored in the browser.	Until the end of the browser session
Search queries	To perform endpoint searches, selected text can be sent as a search query to the cloud API.	Stored in logs for up to 90 days
Tab and context information	Information about the currently active browser tab is processed to correctly map and display tab-related information and endpoints within the browser extension. This is used to provide tab-related features within the browser extension.	No storage