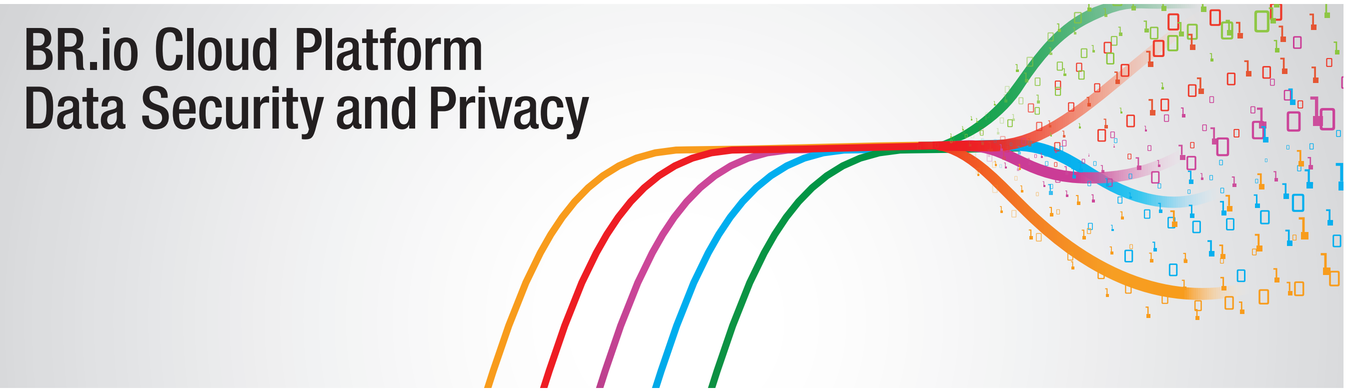
BR.io Cloud Platform Data Security and Privacy



We take data security very seriously and protecting your data is our top priority. We understand that your data belong to you, not us, and we promise to treat it that way. That means designing **BR.io cloud platform** with a security- and privacy-first approach.

How We Treat Your Data

We will use your data only for legitimate and proper business reasons. We will never sell your data to or share it with third parties. **BR.io cloud platform** has no interest in storing your data longer than necessary. Any tracking that we do is anonymous and designed to improve our service and deliver the best possible experience to you.

Our Infrastructure

Your data are safely hosted in SOC-compliant data centers by Amazon Web Services (AWS). Our entire infrastructure is spread across at least two availability zones (data centers) that are based in the United States. Our software is designed to continue working in the event of a complete failure of an underlying data center.

The operating systems we use are updated on a regular basis to ensure we have the latest software and security patches installed. Our databases have both high availability and backup mechanisms.

We use end-to-end encryption technology used by most financial and healthcare institutions. The HTTPS/TLS protocol is used to protect data in transit and a 256-bit advanced encryption standard (AES) is used to protect data at rest. That means your data is protected from the moment it leaves your instrument or computer until it is stored on the **BR.io cloud platform**.

Access to **BR.io** requires a valid email address and a strong password. Login credentials are one-way hashed using a strong hashing algorithm. Not even our staff can see or access your password. We have also implemented a session management feature to automatically lock accounts after periods of inactivity.

You can find the AWS security and compliance documents at the following links:

aws.amazon.com/compliance
aws.amazon.com/security

Security Audit

Our infrastructure is regularly tested for security vulnerabilities by independent security researchers and hardened to enhance security and protect against attacks.

Our Security Policies

We require all employees to attend mandatory data privacy and security training every year. We follow the principle of least privilege and we allow access to customer data on a need to know basis. This means only the Bio-Rad employees who are required to support a specific customer's needs will have permissions and access rights to view that customer's data. We require all employees to undergo a thorough background check that verifies their employment/education, criminal, and credit background before they begin employment. We also require all contractors to sign and agree to a nondisclosure agreement before we conduct business with them.

Email us at **dataprivacy@bio-rad.com** if you have additional questions. In addition, we make proactive efforts to complete appropriate security questionnaires for customers or prospective customers upon request.

BIO-RAD