Your brand is safe with us

Bynder's security and privacy commitment to you and your data

As a globally deployed SaaS provider, Bynder deals with legislation from many parts of the world. We pay close attention to the confidentiality, integrity, and availability of your data and the business continuity of its operations. Bynder is built on a reliable infrastructure that provides enhanced privacy, greater security, and out-of-the-box business continuity; making strong information security a crucial feature of our product.

Our certifications

- ISO 27001:2013, ISO 27018:2019, & ISO 22301:2019 certified: annual independent, third-party ISO audits for locations and product.
- HIPAA compliant: to ensure we safeguard medical information and sensitive patient data.
- PCI-DSS compliant: The Payment Card Industry Data Security Standard (PCI-DSS) to protect information about people, and their payment details, used on any online platform.

- GDPR & CCPA compliant: fully aligned with EU, UK, and US data protection laws including, but not limited to, the latest GDPR and CCPA legislation.

Hosting partner AWS

Bynder has combined security measures with our hosting partner Amazon Web Services (AWS) to ensure that data stored within Bynder is safe from leaks and security breaches. AWS guarantees 99.9% durability on all object storage and offers security that scales with your usage.

Technical measures

- Publicly available responsible disclosure policy. More details: https://www.bynder.com/en/legal/responsible-disclosure-policy/
- Dedicated security tooling for vulnerability management, Open Source library vulnerabilities, and many more.
- Annual penetration testing (based on OWASP top 10) from an independent third party.
- We encrypt data using strong algorithms and encryption keys where possible.
- A well defined secure software delivery lifecycle (SSDLC), aligned with the ISO standards, so that only secure and reliable software gets released to production.
- In-product functionalities like the Waiting Room, permission and access rights, and SSO/MFA capabilities enforce an extra level of security for Bynder users and administrators.

Organizational measures

Bynder's very own Information Security team is led by our CISO and it includes multi-disciplined security officer(s) and ethical hacker(s) who validate the security of Bynder products on a daily basis.

Bynder employees receive regular training and refreshers on security measures to ensure information security is a collective responsibility of Bynder management and staff.

Bynder is audited, at least, annually by an independent third party to make sure the Information Security Management System (ISMS) and the Business Continuity Management System (BCMS) are up to date and correctly applied.

Learn about the security measures that Bynder takes to manage the confidentiality, integrity, availability, and continuity of customer data. https://www.bynder.com/en/security/