Je merk is veilig bij ons

Bynder’s veiligheid en privacy belofte voor jou en je data

Als wereldwijde SaaS-aanbieder houdt Bynder zich bezig met wetgeving uit vele delen van de wereld. Wij besteden veel aandacht aan de vertrouwelijkheid, integriteit en beschikbaarheid van je gegevens en de bedrijfscontinuïteit van de bedrijfsvoering. Bynder is gebouwd op een betrouwbare infrastructuur die zorgt voor meer privacy, meer veiligheid en out-of-the-box bedrijfscontinuïteit; een sterke informatiebeveiliging is dan ook een cruciaal onderdeel van ons product.

Onze certificeringen

- ISO 27001:2013, ISO 27018:2019 and ISO 22301:2019 gecertificeerd: jaarlijkse onafhankelijke ISO-audits van derden voor locaties en producten.
- HIPAA compliant: om ervoor te zorgen dat we medische informatie en gevoelige patiëntgegevens veiligstellen.
- PCI-DSS compliant: De Payment Card Industry Data Security Standard om informatie over mensen en hun betalingsgegevens te beschermen, gebruikt op elk online platform.

- GDPR & CCPA compliant: volledig in overeenstemming met de gegevensbeschermingswetgeving van de EU, het VK en de VS, met inbegrip van, maar niet beperkt tot, de meest recente BBPR- en CCPA-wetgeving.

Hosting partner AWS

Bynder heeft samen met onze hostingpartner Amazon Web Services (AWS) beveiligingsmaatregelen getroffen om ervoor te zorgen dat de gegevens die binnen Bynder worden opgeslagen, veilig zijn voor datalekken en inbreuk op de beveiliging. AWS garandeert 99,9% duurzaamheid op alle objectopslag en biedt een beveiliging die schaalbaar is met je gebruik.

Technische maatregelen

- Verantwoordelijk openbaarmakingsbeleid. Lees hier meer details.
- Specialistische beveiligingstooling voor kwetsbaarheidsbeheer, kwetsbaarheden in de Open Source Library en nog veel meer.
- Jaarlijkse penetratietesten (gebaseerd op OWASP top 10) van een onafhankelijke derde partij.
- We versleutelen data met behulp van sterke algoritmen en encryptiesleutels waar mogelijk.
- Een goed gedefinieerde veilige software delivery lifecycle (SSDLC), afgestemd op de ISO-normen, zodat alleen veilige en betrouwbare software wordt vrijgegeven voor productie.
- In-product functionaliteiten zoals de Waiting Room, toestemming en toegangsrechten, en SSO/MFA mogelijkheden voor een extra niveau van veiligheid voor Bynder gebruikers en beheerders.

Organisatorische maatregelen

Bynder's eigen Information Security team staat onder leiding van onze CISO en bestaat uit multidisciplinaire beveiligingsmedewerker(s) en ethische hacker(s) die dagelijks de beveiliging van Bynder producten valideren.

De medewerkers van Bynder krijgen regelmatig training en bijscholing over beveiligingsmaatregelen om ervoor te zorgen dat informatiebeveiliging een collectieve verantwoordelijkheid is van het management en het personeel van Bynder.

Bynder wordt ten minste jaarlijks door een onafhankelijke derde partij geaudit om er zeker van te zijn dat het Information Security Management System (ISMS) en het Business Continuity Management System (BCMS) up-to-date zijn en correct worden toegepast.

Lees meer over de beveiligingsmaatregelen die Bynder neemt om de vertrouwelijkheid, integriteit, beschikbaarheid en continuïteit van klantgegevens te beheren.