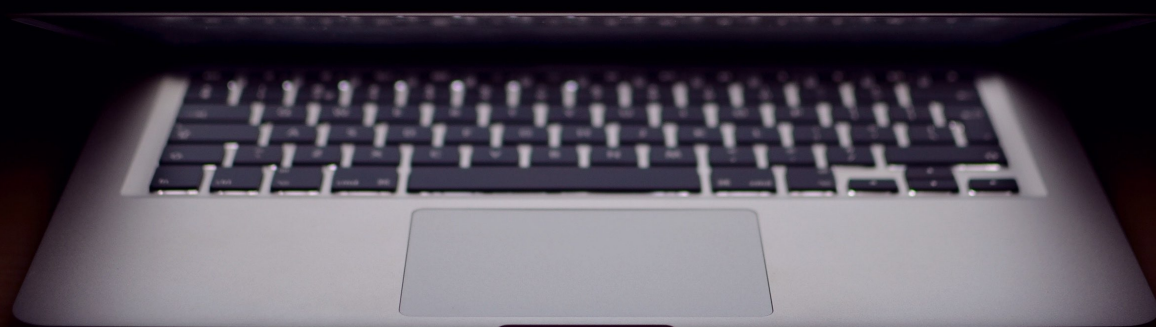




Privacy-first design:

# A Bynder security e-book



Privacy-first design: A Bynder security e-book

# Introduction

As an ISO 27001:2013 certified SaaS pioneer, Bynder is built on a reliable infrastructure that provides enhanced privacy and greater security when compared with many traditional on-site solutions.

Bynder is committed to offering a confidential cloud-based home for company content. As such, Bynder's trusted globally-accessible solutions are fully HIPAA compliant and underpinned by strict policies that are fully aligned with EU data protection laws. Furthermore, Bynder's combined security measures with our hosting partner Amazon Web Services (AWS) ensures that data stored within Bynder is safe from leaks and security breaches.

This detailed white paper outlines how serious we are about ensuring the confidentiality, integrity and availability of our customers' data at all times, and explains why you can put your trust in Bynder.

Introduction	2
Organizational context	4
Information security management system	
Why infosec is our top priority?	
Certifications and compliance	5
ISO Certification	
HIPAA	
PCI-DSS	
GDPR compliance	
Our Suppliers	7
Amazon Web Services (AWS)	
NewRelic	
Monitoring and Review of Supplier Services	
What do we store, and why?	9
Your assets	
Waiting room	
Retrievability through cold storage	
Permission management	
Shared with nobody	
Organizational Measures	11
Training	
ISMS Monitoring	
Regulatory compliance	
Audits	
Process control and supplier relationships	
Technical Measures	13
Secure development environment	
Penetration testing	
Automated Updates	
Backups	
Data encryption	
Vulnerability management	
Dealing with breaches	15
Notification procedures	
About Bynder	16

# Organizational context

Bynder is the leading cloud-based marketing software that allows users to easily create, find and use their company content within a highly secure and centralized portal. In addition to respecting and protecting our customers' privacy, our focus on convenience means our product combines our 24/7 safeguarding through a strict roles and profiles system with a scalable SaaS product that grants our users anytime-anywhere access to their assets.

## Information security management system

Bynder's information security management system (ISMS) is a system designed to determine what external and internal issues are relevant to Bynder's goal of providing a solution for managing, improving and growing marketing and branding processes. Our ISMS is documented in a lengthy text that outlines information security (infosec) processes in the Bynder SaaS product, implementation services, support services and professional services.

## Why infosec is our top priority?

As a globally deployed SaaS provider, Bynder deals with legislation from many parts of the world and, therefore, has to pay close attention to its confidentiality, integrity, and availability of customer data. In addition to legislative requirements, our customers demand this from the product and services we deliver, thereby making strong information security a crucial feature of our product.

Bynder's ISMS not only ensures continuity of our business but also minimizes any possible damage that information security incidents could cause to our customers. Our ISMS implements both proactive and reactive controls, providing customers with a comprehensive, secure and trustworthy platform for the storage of their digital assets. We closely monitor and periodically update our ISMS documentation to make sure that it reflects the state of the art and meets future challenges.



# Certifications and compliance

Because Bynder respects and protects all of our customers' privacy, we think it is important to invest in security certifications on the one hand and develop best practices internally, on the other hand, as ways to ensure that we provide a compliant and confidential service. Further to this, we conduct periodic audits and rigorous internal testing to verify that we stay at the bleeding edge of tech security. We see this effort as well spent in order to earn our customers' trust and confidence in the confidentiality and reliability of the product.

## ISO Certification

ISO 27001:2013 is a well-known information security standard that places great emphasis on measuring and evaluating how well an organization's ISMS is performing. Bynder earned its ISO certification with our robust ISMS, which manages our information security—and that of our clients'—and safeguards all information and assets to a verified global standard. We also conduct annual ISO audits for all of our premises, as a way of ensuring that we keep our certification but also continuously improve our processes.. We are also actively working towards new certifications and compliance standards like ISO 27018:2014, ISO 22301:2012 and more.

## HIPAA

HIPAA is the compliance standard designed to complement United States legislation for the safeguarding of medical information and sensitive patient data. As of May 2016, Bynder is compliant with all HIPAA security standards following a Coalfire assessment. Bynder maintains its HIPAA compliance by monitoring processes on an annual basis and adjusting where necessary to ensure that our processes are always up to date.

*“At Bynder, we understand the importance of data security, especially for our clients who work in highly regulated industries. For our clients in the pharmaceutical and healthcare industry, ensuring all of their vendors and software meet every compliance and regulatory requirement is imperative.”*

Bas Groeneweg, Information Security Office at Bynder

## PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) v3.2 is meant to protect information about people, and their payment details, used on any online platform, such as websites, e-commerce platforms, and other online services. Compliance with the world-renowned PCI-DSS completely matches Bynder's priority to provide an easy-to-use trustworthy system that safeguards all of your digital assets against theft or loss and maintaining the same security standards you would have for your credit card details, applied to digital assets that are stored in your portal.

## GDPR compliance

The General Data Protection Regulation (GDPR) aims to strengthen and unify data protection for all European Union (EU) data subjects (i.e. citizens and residents). GDPR, and its extraterritorial application, improves on the old Data Protection Directive 95/46/EC by strengthening rules on citizen rights, corporate obligations and international data transfers. By implementing GDPR standards here at Bynder, it gives us and our users, peace of mind knowing that we meet the latest regulatory requirements but most importantly, we put the privacy of our customers and their assets at the highest level.

# Our Suppliers

Because Bynder is a Software as a Service solution, we take full responsibility for the hosting of your brand portal. This means that you never have to worry about the complex hosting and security aspect of having a hosted brand portal. Before partnering with any third-party suppliers, we carry out an in-depth assessment of their security and privacy practices to ensure that they provide the same high level of security and confidentiality terms we offer our customers. Our current suppliers are:

## Amazon Web Services (AWS)

Bynder chose online storage partner Amazon Web Services (AWS)—trusted by corporations and governments around the world—because it is renowned for rigorous online and physical security measures. AWS also guarantees 99.999999999% durability on all object storage and offers security that scales with your usage. AWS's data server structures are designed to minimize the impact of global operational disruptions. AWS stores all of Bynder's customers' data in highly secure data centers that are staffed around the clock by specially trained security guards. Since authorized access is granted strictly on a need to know basis, Bynder and unauthorized persons are prevented from accessing customer data without their consent. Read more about AWS' security, [here](#).

## NewRelic

Leaders in the cloud security community, NewRelic is a Tier III, SOC2 certified data center located in Chicago, Illinois. It boasts fully redundant power backup systems, fire suppression systems, security guards and biometric authentication systems. Bynder chose to work with NewRelic after being impressed by their transparency with respect to their policies and systems, as well as the leading security technologies and procedures they use to safeguard customer information from unauthorized access, use or disclosure. Read more about NewRelic's security, [here](#).

## Monitoring and Review of Supplier Services

When working with suppliers, Bynder's security team continually monitors their product performance and security levels. If we come to believe that the service is not what we expected, or that the supplier's way of working is not optimal for our customers, this will be reported to a member of the Board or the Chief Information Security Officer (CISO). A new supplier can then be selected, and the list of approved suppliers with excellent service will be updated to ensure that all Bynder employees know who we work with.



# What do we store, and why?

Bynder offers a confidential cloud-based home for digital assets by securely storing customer content and preventing against unauthorized access.

## Your assets

Bynder supports the majority of standard asset formats and supports the following files for previews:

<b>Supported Containers</b>	jpg, jpeg, pdf, png, gif, tiff, bmp, svg, psd/psb, eps, wmv, mp4, mpeg/mpg, mov (excl Apple prores), avi, flv, vob, mkv, mxf, m4v, f4v, 3gpp, 3gp, ogv, ts, mts, m2ts, 3g2, m2v, webm, .indd (only preview), .ai (PDF-compatible)
<b>Supported Video Codecs</b>	MP4, H264, AAC, TS, WebM, VP8, Ogg Vorbis audio
<b>Supported Audio Codecs</b>	wav, mp3, ocm, wma, m4a, ogg, aiff, aif, m4r

## Waiting room

To regulate file upload access and rights to nonaccount owners of your DAM platform, Bynder offers an extra level of security with the waiting Room functionality. This feature limits access and upload rights for users that do not have login credentials and enables our customers to maintain control over the content that is uploaded to their asset bank. They can deliver assets to the waiting room where an administrator or content manager can review the asset, and subsequently choose whether to accept or refuse it. Assets that are not accepted will not be moved to the asset bank.



## Retrievability through cold storage

Bynder offers a cold storage option based on AWS Glacier, which provides a low-cost way to store data not used on a regular basis. Retrieving and downloading archived files varies from 2-4 hours.

## Permission management

A Bynder Administrator or Regular user can choose to set different permissions for various profiles based on a range of criteria or variables. Single Sign-On As an added level of security, Bynder offers Single Sign-on (SSO)—a property of access control for multiple, but independent, related software systems. With this feature, a user can log in with a single ID to gain access to a connected system without the need for different usernames or passwords, or in some configurations, seamlessly sign on for each system. IT System Administrators can enjoy greater security controls and can also remove and revoke rights directly from the Active Directory. Bynder prefers operating with a client's Active Directory Federation Services (ADFS) based on Security Assertion Markup Language (SAML) 2.0 as it provides the client with full control over all its Bynder users. Password Security All passwords are hashed using NIST-approved algorithms (PBKDF2) where possible, with the result that it is not feasible to reverse the password

## Shared with nobody

Bynder has a strict policy relating to the management of all customer data. Customer data that is given to us for storage in the product to us is only stored in Bynder and never shared elsewhere. A common concern among our customers relates to how their data is used or shared in isolated (non-network) systems. Please be assured that, apart from the information our customers choose to store in their environment, Bynder only stores the following user information:

- First name
- Last name
- Email address
- Actions within the Bynder system
- Any (arbitrary) information the SSO provider chooses to share upon login

# Organizational Measures

Internally, Bynder develops and disseminates information security standards that provide its personnel with an overview of our security requirements, as well as a description of the controls in place to ensure that these standards are met.

## Training

Information security is a collective responsibility of Bynder management and staff. To ensure that all employees are educated and aware of the applicable security standards, Bynder organizes training sessions for new and existing employees. These training sessions include in-person talks, online tutorials and continuous awareness activities, all of which ensures that the documentation on security is read and understood company wide.

## ISMS Monitoring

Bynder monitors, measures, analyses and evaluates its performance on an annual basis, which includes internal audits, risk treatment and management reviews. With rigorous monitoring, we aim to continue improving our ISMS to identify nonconformities and correct any errors.

## Regulatory compliance

Bynder keeps track of legislative and contractual requirements for all customers and regions in which we offer our product and services. We follow the European Union Data Protection Directive EC/46/95 and data protection and privacy laws in every country where we have offices— the Netherlands, United Kingdom, Spain, United States, and UAE. From May 25th, we will be GDPR compliant. Also, we have established our core data processing clusters in Frankfurt as a commitment towards customer data protection in accordance with European Union law.

## Audits

Bynder is audited at least once a year by an independent third party to make sure the ISMS is up to date and correctly applied. This is part of maintaining our ISO27001 certification.

## Process control and supplier relationships

Security protocols are also implemented with our suppliers to ensure that they do not pose an information security risk. Following a detailed supplier review conducted by a member of the security and legal team, all suppliers are classified as either high- or low-risk. The review verifies that any customer information handled by a supplier satisfies Bynder's security policies.



# Technical Measures

## Secure development environment

Establishing a secure environment for system development and integration efforts is the first line of defense in software development. For this reason, Bynder's development environment is set up entirely on local servers and is only accessible from within our internal network or via VPN. Additionally, external credentials are isolated from production resources during development in order to guard against accidental alteration of data. To ensure that every feature update adheres to our strict security measures, we conduct secure development practices in which trained personnel test each feature for potential security issues prior to release. This is executed through peer code reviews by developers trained to abide by a best practice checklist, which enforces the correct use of secure development guidelines.

## Penetration testing

Bynder uses an automated vulnerability scanner for continuous automated scanning and a third party for annual penetration testing. This helps us to proactively identify potential security risks and mitigate them with the best remedies, in addition to creating safeguards for future vulnerabilities. To protect client data and to circumvent the Intrusion Detection System (IDS) already in place, we set up a duplicate environment on separate servers and allocated specific time slots in which the application will be pen-tested.

## Automated Updates

Our servers are based on Ubuntu LTS and managed through fully-automated systems. All base images are rebuilt on a daily basis, and every release and scaling operation of our product is built from scratch on virtual servers using these base images. Subsequently, all of our servers are supplied with the latest security patches.

## Backups

Bynder's 99.99999999% data durability will keep your files safe. All assets uploaded are backed up every day to Glacier storage. In the (unlikely) case of a catastrophic system-wide failure, we can perform a backup restore within one business day.

- The Bynder team secures backups of all data and code in the following manner:
- Incremental backups of all uploaded assets (once every 24 hours).
- Snapshot of the database every 24 hours with a retention of up to 30 days.

## Data encryption

Securing and maintaining cryptographic keys is essential to ensuring the privacy of customer data and personally identifiable information. For this reason, Bynder forbids the use of unproven and unqualified systems that have not yet been peer reviewed by cryptographic experts.

We encrypt data at rest (AES) and in transit (TLS1.2) using strong algorithms and encryption keys where possible. We control data and encryption on server side and data doesn't get encrypted before it is transmitted to our servers, other than the TLS (https) connection that our client uses.

Data on Amazon S3 is encrypted with one key per "bucket", or storage container. Data in external transit is encrypted with the domain specific TLS keys (\*.getbynder.com, \*.bynder.com and brand.client.com, etc), whereas data in internal transit is encrypted with a custom TLS private key that Bynder generates.

## Vulnerability management

The development team monitors software vulnerabilities. If a software used by Bynder contains vulnerabilities, then automated updates or—when necessary—manual updates will be installed to remediate the issue as soon as possible. Significant software changes are always tested beforehand. When a vulnerability has an impact on a customer's confidentiality, integrity or availability, the customer will be updated in accordance with the Bynder notification protocol.



# Dealing with breaches

## Notification procedures

Minor incidents that pose no significant threat are resolved in the regular release schedule, and notifications are sent upon release of the mitigation. Threats that pose an immediate threat to confidentiality, integrity or availability are resolved as soon as possible, and notifications are sent directly. Notifications will contain an impact analysis. Notifications will contain an impact analysis and are sent to affected customers without undue delay.





# About Bynder

## Create, find and use your content when you need it

Bynder is the fastest way to professionally manage digital files. Its award-winning digital asset management (DAM) platform offers marketers a smart way to find and share creative files such as graphics, videos and documents.

Thousands of brand managers, marketers and creatives from global organizations like PUMA, innocent drinks and KLM Royal Dutch Airlines use Bynder to organize company files; edit and approve projects in real time; auto-format and resize files; and make the right content available to others at the click of a button.

Founded in 2013 by CEO Chris Hall, Bynder has seven global offices located in The Netherlands, USA, Spain, UK and UAE. For more information, visit [www.bynder.com](http://www.bynder.com) or follow Bynder on Twitter @Bynder.



[www.bynder.com](http://www.bynder.com)