PhotoShelter | Brands

How PhotoShelter Secures Your Data

Our Dedicated Approach to Your Data Protection & Compliance

Contents

3 Introduction

4 Shared Security Responsibility Model

5 How PhotoShelter Stores Your Data

6 PhotoShelter’s Data Centers

8 How PhotoShelter Protects Your Data

9 Data Loss Prevention & Safety Measures

10 Disaster Recovery

11 Identity & Access Management (IAM)

12 Encryption

13 PhotoShelter’s Commitment to Compliance

22 Contact Us

Andrew Fingerman

CEO of PhotoShelter

Introduction

PhotoShelter is a market-leading provider of digital asset management solutions.

We help marketers and creatives organize, manage, distribute, instantly share, and collaborate seamlessly on digital content.

With 5+ billion assets securely managed and nearly 100 million annual downloads, PhotoShelter helps thousands of organizations worldwide in sports, education, travel & hospitality, healthcare, arts & media, and more, improve team productivity, drive revenue growth, and protect their brand.

Your data security is our priority. PhotoShelter is committed to providing you with data transparency, privacy, and security. That's why leading brands and businesses trust PhotoShelter to protect their assets. Here's how our team delivers on our commitment to ensure your assets remain protected and compliant.

PhotoShelter's security team is responsible for evaluation and enforcement of the information security requirements contained herein.

For more information, please contact: security@photoshelter.com.

Shared Security Responsibility Model

Photoshelter is built to work alongside your other IT security measures to keep your data safe. We share security and compliance responsibilities with your IT department to ensure you have a fully managed security system in place for operational efficiency and enhanced protection.

PhotoShelter's Responsibility

PhotoShelter is responsible for protecting the infrastructure that runs all of the services offered on our proprietary owned-and-operated private cloud.

IT's Responsibility:

Deciding & Managing Your Company's Encryption Options

Your IT department chooses your company's encryption options for your browsers and networks. PhotoShelter supports the latest available options and defaults to the strongest available.

Keeping Your Own Server & Laptop Up to Date with Security Patches

Please ensure that you are applying the latest available updates and security patches so that you are utilizing the latest protection measures available to you.

Identity Access Management and Asset Classification

You decide how to classify your assets as your team sees fit and apply appropriate permissions depending on who you want to access your assets.

How PhotoShelter Stores Your Data

Security is built into PhotoShelter's DNA. We maintain all our customer data on our powerful, proprietary owned-and-operated private cloud. We don't rely on third-party cloud solutions.

14T+

bytes of data stored

11M+

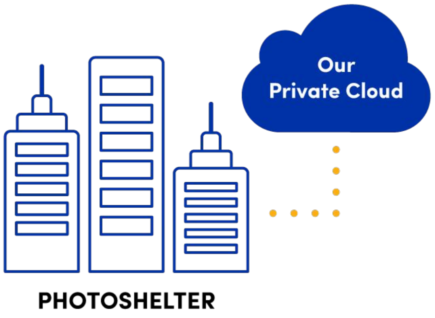
users on our servers

100%

object durability

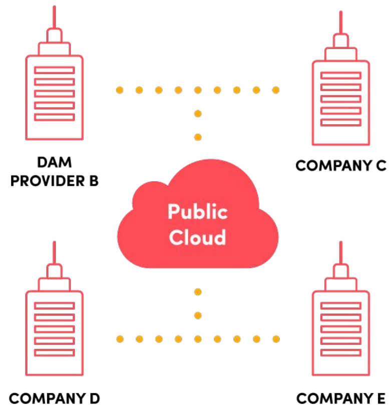
Our system is unique in the marketplace in both security and performance. **We have designed every layer specifically to handle bulk amounts of digital media quickly, efficiently, and securely to serve brand and marketing teams, and professional photographers alike.**

Our private cloud*



*PhotoShelter's private cloud is only used by PhotoShelter customers, whereas other providers that use public cloud services such as AWS, store their customer data in a shared public cloud environment.

Public cloud



Our platform is available only to the customers it serves and fully independently of any commercial cloud platform. The durability of our system is unparalleled by commercial public clouds, including Amazon S3 and Google Cloud. Our own proprietary system also allows us to control costs to ensure that third-party storage price increases do not impact our customers.

Since our beginning in 2005, PhotoShelter has never had a security or privacy breach or lost a single customer file – echoing our long-standing commitment to protecting your data.

PhotoShelter's Data Centers

PhotoShelter operates its private cloud across three geographically-distributed data centers. This approach lets us process your data closer to you, lowers cybersecurity risk, reduces network latency, and increases download/upload speed.

PhotoShelter uploads four copies of your data to at least two geographically-distributed data centers and we run automated data recovery tests every week.

Multiple data centers also allow us to put robust data and disaster recovery measures in place. For example, in the event of a natural disaster, we seamlessly and automatically shift data to another data center so that you and your team can keep working, uninterrupted.

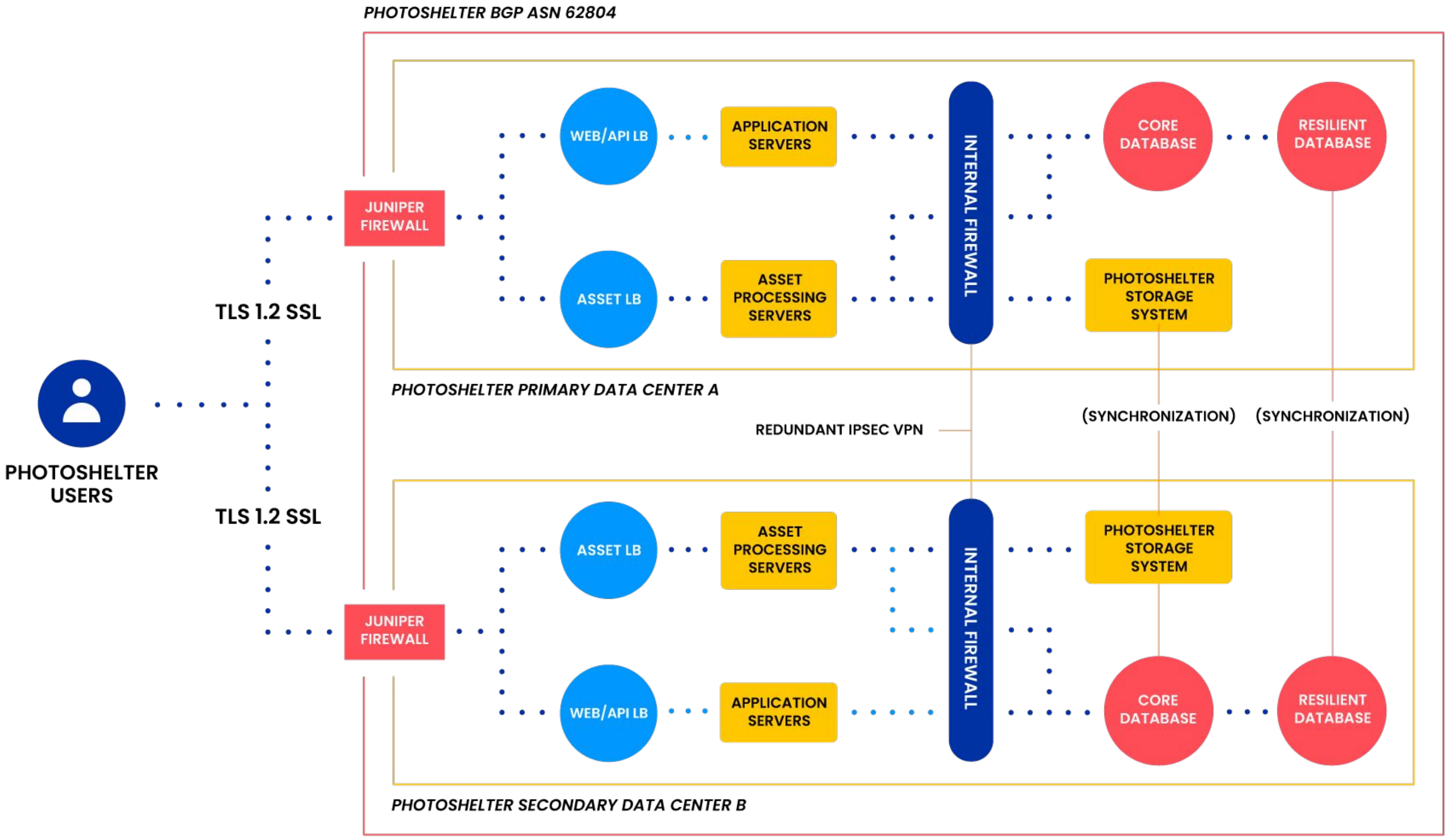
PhotoShelter operates primary data centers in the United States (New York and California) and the United Kingdom.

Additional data caching/acceleration takes place in the United States (New Jersey, Georgia, Florida, Texas, Illinois, California, and Washington), United Kingdom, France, Netherlands, Germany, Singapore, Korea, Japan, and Australia.

PhotoShelter's data center locations: New York, California, and the United Kingdom

Your Data Through PhotoShelter: A Journey

Here is an example of how your data flows from your PhotoShelter account through our systems at our data centers to maintain the utmost levels of security:



The process that occurs in data center 1 is mirrored in data center 2. That way, a copy of your data is always safe and accessible on one of our servers.

How PhotoShelter Protects Your Data

1

24/7 Monitoring

PhotoShelter's platform is managed 24/7 by our DevOps team. Current status is available at https://photoshelter.status.io/ Security incidents or concerns can be raised directly to security@photoshelter.com.

2

Change Management

Any change to our infrastructure or software is recorded and tracked using an **internal ticketing system**. Technical Support can be reached directly via email at support@photoshelter.com.

3

Downtime: Planned

If a change requires platform downtime, **maintenance is performed outside of normal business hours** to the best of our ability, and communication is made to customers in advance.

4

Downtime: Unplanned

In adherence to our incident response policy, **we update and maintain our status page** (https://photoshelter.status.io/). Impacted customers receive a notification within 48 hours of discovery via email.

Data Loss Prevention & Protection Measures

PhotoShelter's data centers are SOC 2 Type 2 / ISO 27001 compliant and hold audit reports or certificates for each data center. Documentation can be provided under an NDA.

Data Loss Prevention Methods

- SHA checksums are calculated for your data before it is written to our distributed storage system.
- Checksums are verified for every read and write of data stored in our system.
- Checksum failures are automatically corrected by fetching known good copies.
- Checksums are regularly scrubbed — at least once a month all content is checked to make sure that the on-disk content matches the original checksum.

Data Protection Methods

- Internal vulnerability scans run daily.
- Automated disaster recovery is run every week that simulates the loss of a full datacenter.
- Annual penetration test is conducted by a third-party.
- All software changes are tested in development environments without user data before deployment to production.
- Antivirus and malware protection is deployed to all PhotoShelter user devices.

Disaster Recovery

PhotoShelter conducts a full annual audit of our Disaster Recovery Plan that includes:

- Failure of each of our primary data centers
- Incapacitation of our development/testing environment
- Full loss of our HQ office
- Loss of our Critical Vendors

PhotoShelter carries Cyber Insurance against cybersecurity events.

PhotoShelter has internal policies that guide Business Continuity and Disaster Recovery. These policies are continuously updated and approved by senior leadership to preserve the reliability and integrity of our services. Specific details are privileged IP and can be shared under NDA.

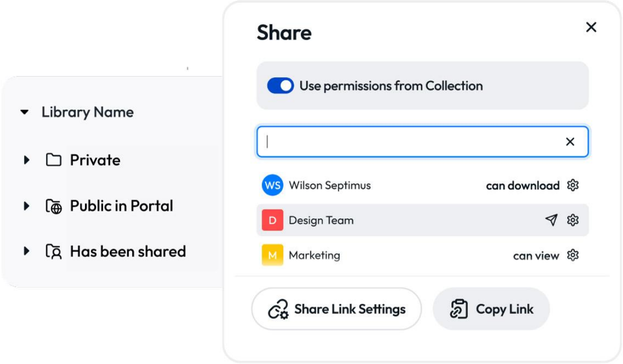
Identity & Access Management (IAM)

PhotoShelter provides deep levels of fine grained access control via group and individual grants.

Individual Access

PhotoShelter customers are given complete control over access to your assets at every level, so you can decide who to share your content with – or not. When you create a gallery from external uploads, it is set to private by default. When you create a gallery in the library, you can set the visibility at the time of creation.

You can easily update permissions and see which collections and galleries are visible or can be downloaded on the portal by looking at the stoplight colors in the library:



- **"Public in Portal"** = Visible without a login.
- **"Has Been Shared"** = Available for individuals and groups that have specifically given permission.
- **"Private Files"** = Only visible to library staff.

Group Access

PhotoShelter supports a single-sign on (SSO) feature that allows you to automatically add employees to a user group as they log in via your Portal, without requiring a new password for each user.

PhotoShelter SSO is primarily built around a SAML2 transport layer to perform the login. SAML2 is widely available with directory services used in enterprise environments:

- SAML 2 Transport layer
- Either SP- or IdP-initiated
- Requires email address, first name, and last name in the assertion

- Optional attribute: group (sorts SSO users into different contact groups)
- HTTPS profile using the POST method

PhotoShelter SSO supports the use of any client-side directory service that can authenticate using SAML2. This is a long and constantly expanding list of enterprise directory services. Below are some of the most common services used by our clients:

- LDAP - many implementations
- Microsoft Active Directory Service (Active Directory, Azure Active Directory, ADFS, and more)
- Oracle
- Shibboleth
- Okta

Encryption

PhotoShelter encrypts your personal identifiable information (PII) (your full name and email address) to ensure it’s unreadable, in order to maintain your privacy. We encrypt this data in two ways:

At rest

Protects your data when it’s stored anywhere. (e.g. on a hard disc or backup media).

- Via AES256x2 or better

End-of-life disks are securely shredded.

In transit

Protects your data when it moves anywhere (e.g. between your computer and our servers.)

- Via TLS 1.2 or 1.3 with SCSV downgrade protection, forward secrecy, and AESGCM/CHACHA ciphers

PhotoShelter's Commitment to Compliance

We understand that you need to select products and services that are both compliant with the latest applicable data protection laws, and use personal data in ways that are compliant.

Here is how PhotoShelter is complying with specific privacy laws and frameworks.

GDPR (General Data Protection Regulation)[1]

Since 2017, PhotoShelter has been fully GDPR compliant. Defense Priorities and Allocations are in place for all contracts and sub-processors. PhotoShelter is in compliance with the GDPR by adhering to the 7 main principles of data protection:

- **Lawfulness, fairness, and transparency** – We use personal data in a way that complies with the law, and in a way our customers and staff expect and have been told about.
- **Purpose limitation** – We only use personal data for the reasons we collected it, and not for something extra or unrelated.
- **Data minimization** – We limit the amount of personal data we collect to what we need. For example, if we only need basic contact details of our customers to run accounts, we don't ask for more information.
- **Accuracy** – The personal details in our records are accurate and kept up to date.
- **Storage limitation** – We only keep personal data for as long as we need it. When we no longer need it, it is securely destroyed or deleted.
- **Integrity and confidentiality (security)** – We make sure that the details of our staff and customers are protected and that we can access those details.
- **Accountability** – We hold ourselves accountable for having the appropriate measures in place to uphold these 6 principles.

The controller shall be responsible for, and be able to demonstrate compliance. As of 2023, PhotoShelter's Data Protection Officer is CTO Kathy Carter.

[1] Updated as of July 2023

EU-US Data Privacy Framework[2]

PhotoShelter complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States.

PhotoShelter has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

PhotoShelter's compliance with the Privacy Shield is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

Pursuant to the Privacy Shield Frameworks, EU individuals have the right to:

- Obtain our confirmation of whether we maintain personal information relating to you in the United States.
- Upon request, we will provide you with access to the personal information that we hold about you.
- You may also correct, amend, or delete the personal information we hold about you.

An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under Privacy Shield, should direct their query to **privacy@photoshelter.com**.
If requested to remove data, we will respond within a reasonable timeframe.

Please note that in cases where we are the processor of your Personal Data, we may have to refer you to the controller party to inquire about accessing your data.

We will provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to **privacy@photoshelter.com.**

[2] Formerly EU-US Privacy Shield. Effective October 10, 2023.

CCPA/CPRA (California)[3]

PhotoShelter complies with the CCPA/CPRA by honoring requests from California residents to access, delete, and opt out of sharing or selling their information, including the following:

- The **right to know** about the personal information PhotoShelter collects about them and how it is used and shared;
- The **right to delete** personal information collected from them (with some exceptions);
- The **right to opt-out** of the sale or sharing of their personal information; and
- The **right to non-discrimination** for exercising their CCPA rights.
- The **right to correct inaccurate** personal information that PhotoShelter has about them; and
- The **right to limit the use and disclosure of sensitive personal** information collected about them.

PIPEDA (Canada)[4]

PhotoShelter complies with PIPEDA by getting approval for data collection and use, maintaining appropriate security measures, and providing people with access to their personal information.

What Individuals Have Rights to Request Under PIPEDA

- Ask why PhotoShelter is collecting, using or disclosing their personally identifiable information (PII) (full name, email address, mailing address, zip code)
- Expect PhotoShelter to only collect, use or disclose personal data reasonably and appropriately
- Expect PhotoShelter will not use collected information for any purpose other than that which they have consented
- Know who at PhotoShelter is responsible for protecting their personal information
- Expect PhotoShelter to protect their personal information by taking appropriate security measures, e.g. automated vendor risk scoring
- Expect PhotoShelter to keep personal information accurate, complete and up-to-date
- Obtain access to their personal information and ask for corrections if necessary
- Complain about how PhotoShelter handles their personal information if they feel their privacy rights have not been respected

What PhotoShelter Is Required to Do Under PIPEDA

- Obtain an individual's consent to collect, use or disclose personal information
- Supply an individual with a product or a service even if they refuse consent for the collection, use or disclosure of your personal information unless the information is essential to the transaction
- Collect information by fair and lawful means
- Have personal information policies that are clear, understandable and readily available

[4] Current version: in force since June 21, 2019

HIPAA (Health Insurance Portability and Accountability Act)

Our flexible permissions capabilities allow you to keep assets locked down for private access so that you can manage your library in a HIPAA compliant manner. We have many clients in the healthcare field who use and trust PhotoShelter for Brands for this very reason.

Ways PhotoShelter supports HIPAA compliance:

- PhotoShelter uses a default Zero Trust security profile to authenticate users, and can be integrated into your organization's SSO to ensure that access is granted to the correct people.
- Assets stored within PhotoShelter can be set to private viewing that does not allow them to be viewed externally. These detailed permissions allow you to use PhotoShelter in a HIPAA compliant manner.

PhotoShelter helps you maintain HIPAA compliance by following the required protections of **The Security Rule**, which establishes standards for the protection of health information that is held or transferred in electronic form, which is known as e-PHI.

Risk Analysis and Management

PhotoShelter conducts an annual risk analysis of our systems to:

- Evaluate the likelihood and impact of potential risks to data in our system
- Implement appropriate security measures to address the risks identified in the risk analysis
- Document the chosen security measures and, where required, the rationale for adopting those measures
- Maintain continuous, reasonable, and appropriate security protections, which are explained in further detail below

Administrative Safeguards

- **Security Management Process** – PhotoShelter maintains a security management process. The documentation for our security measures can be found on our proprietary network and security statement.

HIPAA (Health Insurance Portability and Accountability Act)

- **Security Personnel** – PhotoShelter maintains a data security team, led by Kathy Carter, our Chief Technology Officer, who is responsible for developing and implementing our security policies and procedures.
- **Information Access Management** – PhotoShelter's system is built with SSO and detailed usage rights management, ensuring that customers who are covered entities are able to limit the use of any materials stored within PhotoShelter to only those people who require access. We rely on our customers to ensure that the materials they are storing in PhotoShelter are shared with the required privacy settings according to their internal HIPAA policies.
- **Evaluation** – PhotoShelter performs regular assessments of how well our security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

- **Facility Access Control** – All PhotoShelter Data Storage facilities limit access to only authorized individuals in 24/7 guarded facilities with biometrics, mantraps and video surveillance systems.

Technical Safeguards

- **Access Control** – PhotoShelter's SSO, centralized user management, and strong sharing, security and reporting tools ensure that only authorized persons access e-PHI. Data at rest in our system is protected via AES256x2 or better encryption.
- **Audit Controls** – PhotoShelter includes activity logs which will allow customers who are covered entities to record and examine access and other activity in any systems that include e-PHI.

HIPAA (Health Insurance Portability and Accountability Act)

Technical Safeguards (Continued)

- **Workstation and Device Security -** PhotoShelter has industry standard or better policies for desktops and mobile devices, as well as a clean-desk policy.

- **Integrity Controls** – We recommend that our customers implement a firewall or "air gap" between their PHI systems and marketing tools like PhotoShelter to help ensure that e-PHI is protected in the primary systems where it is housed.

- **Transmission Security** – PhotoShelter guards against unauthorized access to e-PHI that is being transmitted through our network with data encryption. Data in transit is protected via TLS 1.2 or 1.3 encryption.

FERPA (Family Educational Rights and Privacy Act)

Users are able to take advantage of our flexible permission capabilities to keep assets restricted for data compliance like FERPA.

By setting permissions to “not public” you are able to control exactly who has access to sensitive files such as patient data or images, enabling you to use PhotoShelter in a FERPA-compliant way.

Here you can view our public Privacy Statement and contact information for Right of Removal: https://www.photoshelter.com/support/privacy

Contact Us

We invite you to contact us with any questions or comments regarding your Personal Data or our data practices generally. Please contact us if you have any questions regarding your privacy at: **security@photoshelter.com.**

If you are located in the EU, you can also contact us through our Data Protection Officer:

Data Protection Officer
Kathy Carter
(kathy@photoshelter.com)
Chief Technology Officer