FILECLOUD

General Data Protection Regulation

whitepaper

The General Data Protection Regulation (GDPR) is a broad compilation of rules and requirements aimed at protecting the data privacy of EU citizens.
This regulation was established in May 2018 to replace data protection rules initially laid out in the 1990's.

What is GDPR?

The GDPR or General Data Protection Regulation was passed by the EU in 2016, and all organizations were required to be compliant by May of 2018. According to the official website, GDPR is “the toughest privacy and security law in the world.”

You might think if you don’t work or live in the EU that GDPR doesn’t apply to you; however, these regulations extend to companies that target or collect data of people in the EU.

The actual law is hundreds of pages of regulations that relate to the requirements for privacy. Before we go into some of these requirements, let’s talk about why GDPR was put into place.

FileCloud Privacy Settings:

FileCloud provides GDPR compliance tools for all industries to meet stringent security requirements.

Features like password strength enforcement, SSO login and Active Directory integrations, two-factor authentication, antivirus scanning, ransomware protection, advanced encryption, and granular sharing options ensure only authorized users have access to your data.

Privacy and GDPR

Privacy and control over data has become an increasing concern for governments and regulatory bodies over the years. You’ve probably heard of how Facebook has used personal data. In fact you’ve probably been subjected to those annoying ads that seem to target you directly... or been added to an email or phone list without your permission. That’s where privacy standards come into play.

Privacy concerns didn’t start with the advent of the internet. Privacy laws have been passed for decades. In 1950, the European Convention on Human Rights declared that everyone has a right to privacy. The European Data Protection Directive was passed in 1995 and established minimum requirements for security and data protection, but as the internet was established and data began flying around the web, the need for increased security followed it.

That’s where the GDPR came into play.

Who GDPR Relates to and Penalties for Non-Compliance

The law is fairly clear on who it relates to, with the GDPR website saying:
"First, if you process the personal data of EU citizens or residents, or you offer goods or services to such people, then t**he GDPR applies to you even if you're not in the EU...** Second, the **fines for violating the GDPR are very high.** There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages."

These fines relate to these articles specifically (from the GDPR website):

The basic principles for processing (Articles 5, 6 and 9):

Data processing must be done in a lawful, fair, and transparent manner. It has to be collected and processed for a specific purpose, be kept accurate and up to date, and processed in a manner that ensures its security. Organizations are only allowed to process data if they meet one of the six lawful bases listed in Article 6. In addition, certain types of personal data, including racial origin, political opinions, religious beliefs, trade union membership, sexual orientation, and health or biometric data are prohibited except under specific circumstances.

The conditions for consent (Article 7):

When an organization's data processing is justified based on the person's consent, that organization needs to have the documentation to prove it.

The transfer of data to an international organization or a recipient in a third country (Articles 44-49):

Before an organization transfers any personal data to a third country or international organization, the European Commission must decide that that country or organization ensures an adequate level of protection. The transfers themselves must be safeguarded.

The data subjects' rights (Articles 12-22):

Individuals have a right to know what data an organization is collecting and what they are doing with it.

They also have a right to obtain a copy of the data collected, to have this data corrected, and in certain cases, the right to have this data be erased. People also have a right to transfer their data to another organization.

Paying 4% of global revenue is not something *any* company or organization wants to have to pay, so the question is, **what does the GDPR relate to, and how can organizations ensure they're compliant?**

7 Data Protection Principles

GDPR relates to the processing of data and requires that data be processed according to these seven principles found on their website:

1. **Lawfulness, fairness and transparency:** Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation:** You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization:** You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy:** You must keep personal data accurate and up to date.
5. **Storage limitation:** You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality:** Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability:** The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Security of data is a big part of GDPR compliance. If data can be accessed by anyone, then it's not very secure. The GDPR requires your company to have technical and organizational methods in place as well. According to the GDPR website, these methods can include:

- 2FA
- End-to-end encryption
- Employee training
- A data privacy policy
- Limiting employee access to personal data

If a data breach occurs, companies only have 72 hours to tell the owners of that data—or risk facing penalties.

Privacy by design and default

According to the GDPR website, “From now on, everything you do in your organization must, ‘by design and by default,’ consider data protection. Practically speaking, this means you must consider the data protection principles in the design of any new product or activity.”

There are many requirements when it comes to processing, storing, or using personal data that MUST be followed to remain GDPR compliant. One of the biggest requirements is that consent must be obtained and “freely given, specific, informed and unambiguous.” It also must be in plain language (i.e., you can’t complicate it with legalese).

Data Protection Officers

Most companies are not required to have a DPO or data protection officer other than in a few specific cases, but it can be helpful to have a compliance/data protection officer who is in charge of making sure you’re compliant.

Data Subjects Rights

When it comes to rights for those who are data subjects, there are **8 rights** the GDPR website says that GDPR-compliant organizations must protect, including:

Right to be informed

Right of access

Right to rectification

Right to restrict processing

Right to erasure

Right to object

Right to data portability

Rights in relation to automated decision making and profiling

These might seem complicated, but most of them simply relate to the right to know that an organization has an individual’s data, and the right of the individual to have that data deleted/restricted.
When it comes to GDPR compliance, you can’t just say you’re compliant—you have to show it. If you can’t demonstrate or prove compliance, then it doesn’t count—thus, you’re not compliant. That’s why you need to stay compliant, even as regulations change and shift.

How FileCloud can help you meet GDPR Compliance

In our increasingly online and remote world, companies and organizations can no longer share and store data in one place like an office or filing cabinet. In the early days of the internet, important files were shared via email, but as time went on, users learned how email could be compromised. Without proper encryption, anyone can gain access to data.

This vulnerability poses a major risk, especially when companies have to comply with regulations like GDPR, where data breaches mean more than a loss of a client – they could also include steep monetary fines and lawsuits.

That's why many organizations have turned to Enterprise File Sync and Sharing (or EFSS)—software that allows organizations to securely store and share files and folders. As various compliance regulations came into effect, EFSS solutions have often incorporated options for privacy, audits, and granular controls that make compliance much less of a slog than it could be. There are checklists to help with compliance (available on the GDPR website), but using something like an EFSS can be easier.

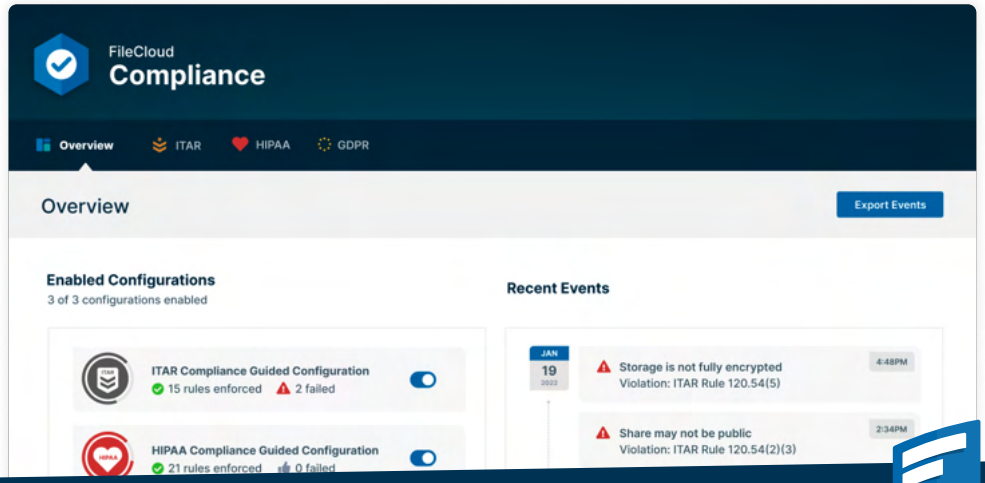
EFSS often have collaboration tools included as well, to improve efficiency and streamline work processes.

FileCloud is a Top EFSS and Compliance Tool

FileCloud is a hyper-secure file sharing and storage solution that enterprise organizations use to store and share their data. FileCloud has always been on top of the latest security and compliance trends, to ensure client data is secure, shareable, and compliant.

In fact, according to Businesswire, FileCloud had the "world's first, availability of General Data Protection Regulation (GDPR) compliance support for organizations utilizing private cloud enterprise file sharing."

From the first, FileCloud has kept on top of compliance regulations and requirements, consistently adding features that help companies become compliant and stay that way. In terms of GDPR Compliance, FileCloud has all the tools necessary to help companies avoid fines and penalties.



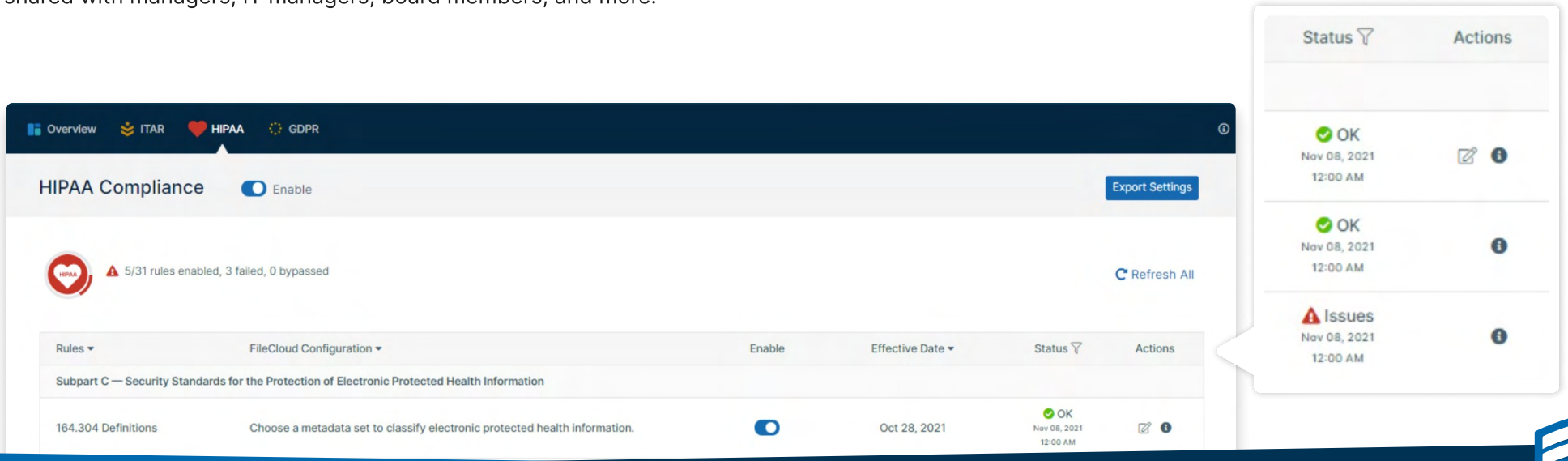
FileCloud's Tools for GDPR Compliance

FileCloud's Compliance Center

FileCloud's Compliance Center combines FileCloud's security and sharing features in one place to aid with compliance. Administrators can follow best-practices, recommendations, and built-in rules for GDPR, but also for HIPAA, ITAR, and more with separate tabs for each regulation.

Admins and users can export settings for each regulation and policy and receive reports on violations so issues can be addressed quickly. Event logs can be saved and reviewed for compliance and audits and easily shared with managers, IT managers, board members, and more.

Admins can explore different compliance configurations in greater detail by clicking on the GDPR, HIPAA, or ITAR tabs within the compliance dashboard. Compliance requirements are listed in a table, along with FileCloud settings that tackle the requirement. There is also a "Status" column that confirms compliance or the number of violations. The "Actions" column gives admins information and editing options which helps admins quickly address issues.

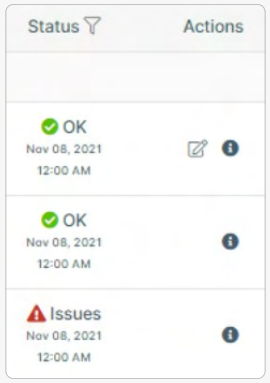


© 2022 FileCloud | www.filecloud.com

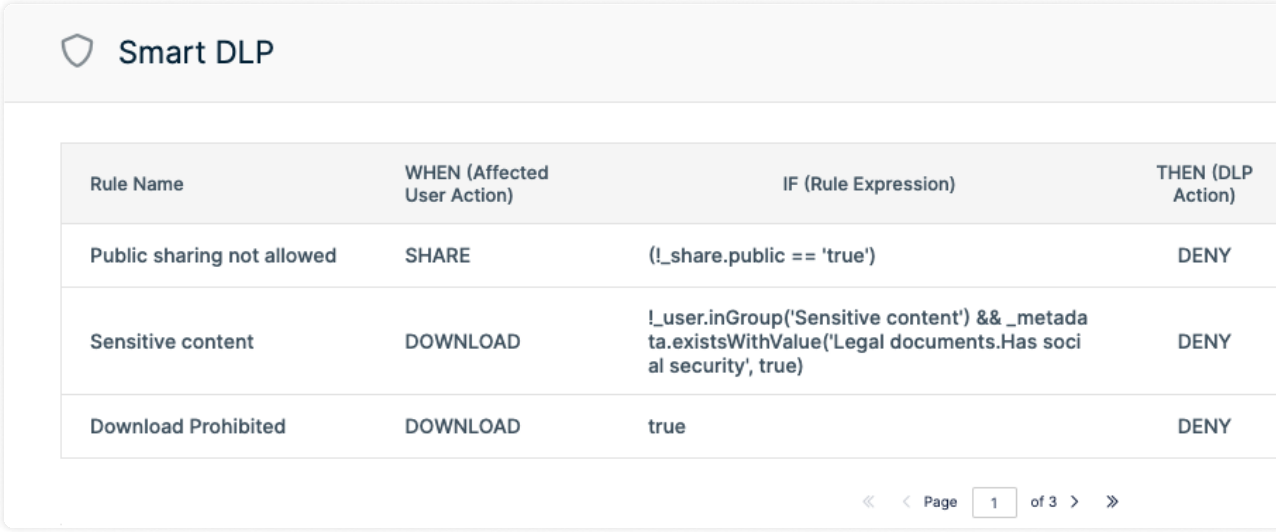
FileCloud's hyper-secure features like custom metadata, Smart Classification, and Smart DLP help organize data and prevent leaks which also helps with compliance.

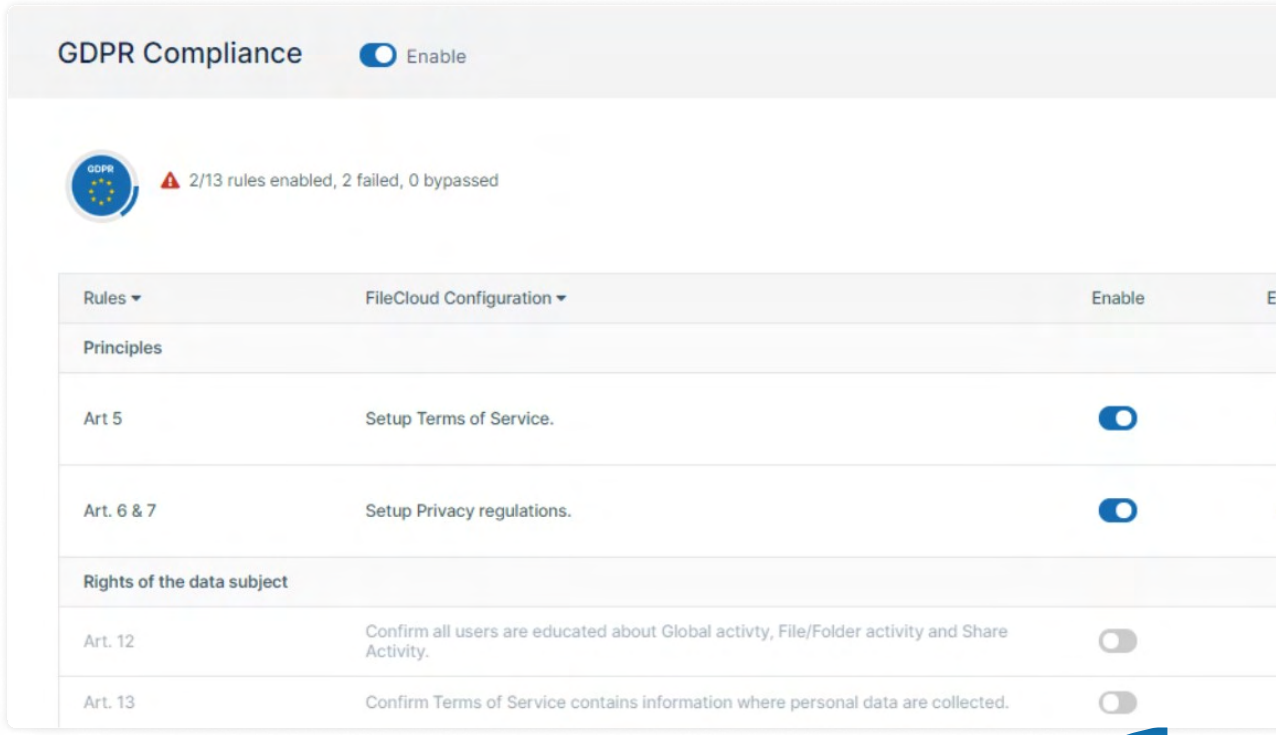
For example, metadata tags can be created for defense articles and technical data, which are then applied to documents using Smart Classification. DLP rules connect with the Classification Engine and helps ensure that files with this metadata set can be shared.

FileCloud's Compliance Center also gives admins SSL, encryption, and audit settings to provide advanced security. Specific rules like "Confirm all users are US residents" are useful prompts for regulations (specifically since the GDPR is in place for EU residents).



Admins also are in total control. If they already have a compliance solution in place, the FileCloud rules can be easily bypassed in the "Actions" column.





FileCloud's Security

One of the things we've covered when relating to GDPR is security and the importance of protecting data.

Evidently, letting data float around without encryption or protections does not conform to GDPR regulations.
That's why FileCloud has advanced, hyper-secure features like:

DRM

Smart DLP

2FA and SSO

Active Directory and NTFS integration

Granular sharing and user permissions

256-bit AES encryption and SSL/TLS protocols to secure data at rest and in transit

From the moment admins access their FileCloud system, the system is secure because of built-in features like:

Automatic anti-virus scanning of files upon upload

Custom metadata and content classification

Unlimited file versioning and file locking

Endpoint device protection

Federated search capabilities

Client application security policies

Comprehensive audit trails

© 2022 FileCloud | www.filecloud.com

Pattern Searching

One helpful tool when it comes to GDPR compliance is FileCloud's built-in pattern searching. Pattern PII Search allows administrators to discover and manage sensitive and protected data. DPOs, compliance officers, and administrators can search for common data types (like email addresses and phone numbers) using the pattern identifier.

In addition to common patterns, there are already-created templates to search for complex patterns, including:

- EU debit card numbers
- Certain EU drivers license numbers/passport numbers
- Banking account numbers
- SWIFT codes

Since GDPR compliance requires that protected information is not shared innapropriately, admins can use these search and pattern templates to immediately identify information that needs to be protected.

User Consent

Consent is an important aspect of GDPR, and GDPR requires that personally identifiable information (PII) has been given consent to be used by those accessing the data.

Thankfully, FileCloud has an easy way to attain this consent, including:

- A privacy setting that asks for explicit consent from the owner of the data
- Once enabled, FileCloud will ask for consent from users while accessing, viewing, or downloading files from FileCloud.
- All PII (personally identifiable information) can be exported in a CSV file in response to user requests to see collected data and how it's been used.

Developing a solid GDPR compliance program demands that IT architects and marketers move beyond the restricted scope of PII to examine the full spectrum of personal data as defined by the EU.

Right to Access

Right to access essentially means companies can't just keep someone's data and then not tell them what they have on them. Within GDPR, people may request any and all information that a company has collected relating to them.

FileCloud has steps in place to make this information easy to find and share.

FileCloud allows an organization's data protection officer/compliance officer or an administrator to search for user data across all file content and activity logs.

Administrators can search for content across all users in the system.

This info is easy to download in a log that can then easily be shared with whoever requested access to the info.

Data Portability

GDPR says that people may request a copy of data for use elsewhere, also known as 'data portability'.

FileCloud allows the export of files in standard formats and activity logs in easily readable files.

Users can move their files easily from FileCloud to any other platform.

Right to Be Forgotten

Another important aspect of GDPR is that people may request that their data be deleted or completely anonymized by the companies who collected the data.
FileCloud aids in this by providing:

- Tools to delete files

- The potential for allowing anonymization of any data that companies possess relating to a user, including activities log.

Data Residency

FileCloud offers data residency options, allowing companies and organizations to pick the region of their choice for storing and processing data. Admins have 100% flexibility regarding where data is stored and processed. This option can be deployed as part of a private or hybrid cloud on an infrastructure that customers control.

FileCloud server is not and never will be a data processer. In FileCloud Online, users can choose where their data is hosted based on their requirements.

Businesses often have to operate under local regulations, which require that data about nations' citizens or residents be collected, processed, and/or stored inside the country due to regulatory, tax, or policy reasons. Data can still be transferred after meeting local privacy or data protection laws, such as giving the user notice of how the information will be used and obtaining their consent.

Data residency refers to where the data is stored by a business or industry body.
Data sovereignty is not just about the data stored in a specific location, but also refers to the laws of the country in which it is physically stored.
Data localization states that data created within certain borders stay within them.

To learn more about data residency around the world, read this blog.

Special User Types (for DPOs)

Companies with over 250 employees should assign a data protection officer (DPO) to overlook GDPR compliance.

FileCloud offers special user types with a subset of administrator tools.

Organizations can create special user accounts for DPOs and auditors to monitor compliance.

You can select a subset of admin features that you want to enable for your DPOs.

FileCloud allows an organization's data protection officer (DPO) or administrator to search for user PII across all file content and activity logs, making it easy to fulfill client requests for information or to implement retention and restriction policies for confidential information.

The DPO should have a comprehensive understanding of the General Data Protection Regulation (GDPR).
Companies having more than 250 employees should assign a data protection officer (DPO) to ensure compliance.

Digital Rights Management (DRM)

Controlling who gains access to files and folders and what happens after they're shared is an important but often overlooked aspect of GDPR compliance. For example, there is a GDPR provision that stipulates files with protected information not be shared with unauthorized people. Thankfully FileCloud has advanced DRM, including options like:

Revoke access even after files have been shared

Create access keys for shared documents

Limit screenshotting/ printing/copying

Set maximum access counts

Restricted viewing mode

Multiple file format support

Create shares with public/private/password protections

Admins can restrict or revoke file access or change view options at any time, which places control over sensitive files back into your hands.

Granular Access Control

Admins can set granular permissions over access, file, and folder permissions for each user. Furthermore, you can restrict features to ensure only the intended users can access, sync, and share data, even within subfolders or specific files in shared folders.

Audit Logs

Admins can generate complete audit trails with detailed reporting on all file transfer and sharing activities. Unchangeable audit logs can be exported in CSV files for ease of governance. The admin dashboard shows all the devices accessing files in real time.

Breach Notifications

GDPR requires that users are notified of any breach. While breach notifications must be handled by the customer, FileCloud has detailed policies and breach plans in place for customer data in FileCloud Online. In FileCloud Server, it's a shared responsibility, but admins are still required to notify the owners of that data of the data breach.

FileCloud and GDPR

FileCloud was created to be a top file sharing, storage, and collaboration tool that allows users to meet compliance standards easily and keep on top of changing standards.
The tools and features highlighted above will help compliance and IT officers get where they need to be and stay that way.

To learn more about FileCloud and GDPR compliance, click the links below.

FileCloud's Compliance Center →

FileCloud and Compliance - FINRA, HIPAA, ITAR, CMMC, GDPR and NIST 800–171 →

GDPR Compliant File and Data Sharing →

GDPR Compliance Platform →

About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.

1M+
USERS

3000+
ENTERPRISES

100+
RESELLERS

90+
COUNTRIES

13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

support@filecloud.com
https://www.filecloud.com

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
REUTERS
US Army Corps of Engineers
NASA
COLUMBUS REGIONAL HEALTH
TOYOTA
Deloitte.

Copyright Notice

© 2022 FileCloud. All rights reserved.
No reproduction without written permission.

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.