GDPR & pCloud

Compliance, privacy, and trust

January, 2026

privacy@pCloud.com

Executive Summary

The General Data Protection Regulation (GDPR) represents a fundamental shift in how organizations approach data privacy and protection. Since its implementation on May 25, 2018, GDPR has established one of the world's most comprehensive frameworks for safeguarding personal data and empowering individuals with control over their information.

At pCloud, we recognize that GDPR compliance is not merely a regulatory obligation but a commitment to respecting the fundamental right to privacy. Our Swiss-based operations, combined with our zero-knowledge architecture and data governance practices, position pCloud as a trusted partner for organizations seeking to exceed GDPR requirements. This white paper provides insights into how pCloud supports your privacy and security objectives.

Table of contents

Understanding GDPR: Fundamentals and Implications

What is GDPR?

The General Data Protection Regulation is a comprehensive legal framework adopted by the European Union and now enforced across all EU member states and the European Economic Area (EEA). Effective since May 25, 2018, GDPR applies to any organization-regardless of where it's located-that collects, processes, or stores personal data of EU residents.

GDPR replaces the 1995 Data Protection Directive and represents a significant evolution in data protection law. Rather than focusing solely on data security, GDPR establishes a holistic framework that emphasizes individual rights, organizational accountability, and transparent data governance. The regulation imposes substantial penalties for non-compliance, reaching up to €20 million or 4% of annual global revenue, whichever is greater.

Why GDPR Matters for Organizations

Organizations subject to GDPR must fundamentally reconsider how they collect, process, and store personal data. The regulation requires them to implement privacy by design, maintain detailed records of data processing activities, and demonstrate compliance through documentation and audits.

For cloud service providers like pCloud, GDPR compliance means implementing robust technical and organizational measures to protect data at every stage of its lifecycle. It also means establishing transparent relationships with customers regarding data processing, implementing mechanisms for individuals to exercise their rights, and maintaining the infrastructure necessary to respond to data subject requests within strict timeframes.

Personal Data Under GDPR

GDPR defines personal data broadly as any information relating to an identified or identifiable natural person. This includes obvious identifiers such as names, email addresses, and phone numbers, but also extends to location data, online identifiers, device information, and any other information that could directly or indirectly identify an individual. Because of this expanded definition organizations need to implement comprehensive data protection measures across all systems and processes that handle such information.

The Seven Core GDPR Principles

GDPR is built on seven fundamental principles that guide how organizations must handle personal data.

1. Lawfulness, Fairness, and Transparency

Data processing must be lawful, fair, and transparent. Organizations cannot process personal data arbitrarily; they must have a valid legal basis for processing. Common legal bases include explicit consent, contractual necessity, legal obligation, protection of vital interests, public task performance, or legitimate interests. Fairness requires that data processing does not disadvantage or discriminate against individuals. Transparency means organizations must clearly communicate to individuals how their data is being processed, who has access to it, and what rights they possess. Privacy notices and data processing disclosures must be written in clear, accessible language rather than legal jargon.

2. Purpose Limitation

Personal data must be collected for specified, explicit, and legitimate purposes only. Organizations cannot collect data for one purpose and later repurpose it for unrelated uses without obtaining fresh consent or identifying a new legal basis. This principle prevents the gradual expansion of data use beyond its original scope. When organizations intend to use data for new purposes, they must assess whether the new use is compatible with the original purpose. If not, they must obtain additional consent or identify an alternative legal basis. This principle ensures that individuals maintain control over how their data is used and prevents organizations from exploiting data collected for one purpose for entirely different applications.

3. Data Minimization
Organizations should collect only the personal data that is strictly necessary for their specified purposes. This principle encourages a lean approach to data collection, reducing both privacy risks and storage costs. Before collecting any personal data, organizations should ask whether the information is truly necessary to achieve their stated objective. This principle reflects the understanding that less data means less risk-fewer systems to secure, fewer potential breach vectors, and fewer data subject requests to manage.

4. Accuracy
Personal data must be accurate, complete, and kept up to date. Organizations are responsible for maintaining data quality and correcting inaccurate information when they become aware of errors. This principle recognizes that inaccurate data can harm individuals-incorrect credit information, wrong employment records, or mistaken identity associations can have serious consequences.

5. Storage Limitation
Personal data should be kept in a form that permits identification for no longer than is necessary for processing. Once data has served its purpose, organizations should delete it or anonymize it so that individuals can no longer be identified. This principle encourages organizations to establish clear data retention schedules and implement automated deletion processes. Even if data is currently secureBy limiting storage duration, organizations reduce their exposure to data breaches and demonstrate respect for individuals' privacy.

6. Integrity and Confidentiality
Personal data must be processed in a manner that ensures appropriate security and protection against unauthorized processing, accidental loss, destruction, or damage. This principle requires organizations to implement technical and organizational measures proportionate to the risks posed by their data processing activities. Integrity and confidentiality protections encompass encryption, access controls, audit logging, employee training, and incident response procedures.

7. Accountability
Organizations are responsible for demonstrating compliance with all GDPR principles. Accountability requires maintaining detailed records of data processing activities, implementing security measures, and being able to demonstrate compliance during audits or investigations.

Implementing GDPR Rights in Practice

1. Right of Access
GDPR grants individuals the right to obtain confirmation of whether an organization processes their personal data and, if so, to receive a copy of that data in a structured, commonly used, and machine-readable format. Organizations must respond to access requests within 30 days.

pCloud provides mechanisms enabling customers to respond to data subject access requests. We can generate reports of personal data stored in customer accounts and provide this information in standard formats. Our systems are designed to facilitate rapid access request responses, helping customers meet GDPR's 30-day deadline.

2. Right to Rectification
Individuals have the right to correct inaccurate or incomplete personal data. When an individual requests correction, organizations must update their records promptly.

pCloud enables customers to update personal data stored in their accounts and provides tools for bulk data corrections when necessary.

3. Right to Erasure
Also known as the "right to be forgotten," this right allows individuals to request deletion of their personal data under certain circumstances. Organizations must delete personal data when it is no longer necessary for its original purpose, when the individual withdraws consent, or when the individual objects

pCloud provides secure data deletion mechanisms that permanently remove personal data from all server locations. When customers delete files or close accounts, we ensure that data is removed from our primary systems and from all backup copies within a reasonable timeframe.

4. Right to Data Portability
Individuals can request that their personal data be transferred from one service provider to another in a structured, commonly used format. This right enables individuals to switch service providers without losing their data.

pCloud supports data portability by enabling customers to export their data in standard formats. Users can download their files and associated metadata, facilitating transfers to alternative service providers if desired. We provide clear guidance on data export procedures and maintain data in formats that are compatible with other services.

5. Right to Object
Individuals can object to the processing of their personal data, particularly for direct marketing or profiling purposes. When individuals exercise this right, organizations must cease processing unless they can demonstrate compelling legitimate interests that override the individual's objections.

pCloud respects objection requests and ceases processing personal data for the purposes to which individuals object.

6. Right to Restrict Processing
Individuals can limit how their personal data is processed, in certain circumstances.

pCloud respects this right and pauses personal data processing when required.

pCloud's GDPR Compliance Strategy

We take security and privacy very seriously. For that reason, we have an ongoing commitment to not only meet GDPR standards but even to exceed them.

1. Organizational Commitment
pCloud's approach to GDPR compliance begins with organizational commitment at the highest levels. Our legal and security teams work collaboratively to ensure that GDPR principles are embedded in every aspect of our operations. As new best practices emerge, we assess the implications for pCloud and implement necessary adjustments to our practices. We recognize that GDPR compliance is not a one-time project but an ongoing commitment which is reflected in our dedicated privacy and security personnel, regular employee training programs, and investment in compliance infrastructure.

2. Privacy by Design
pCloud implements privacy by design principles across our entire platform. Rather than adding privacy protections as an afterthought, we consider privacy implications during the initial design phase of new features and services. When our engineers develop new features, they consider questions such as: What personal data will this feature process? What are the privacy risks? What technical and organizational measures can minimize these risks? How will users exercise control over their data? By asking these questions early, we can design features that are inherently more privacy-protective.

3. Data Residency and Security

pCloud recognizes that organizations subject to GDPR often prefer to keep personal data within the European Union to ensure compliance with data residency requirements and to minimize legal complexities around data transfers. We maintain data centers in the European Union (specifically in Luxembourg) and in the United States (in Dallas, Texas). Customers can choose where their data is physically stored, enabling EU-based organizations to maintain data within EU jurisdiction if desired. This flexibility ensures that organizations can meet their specific compliance requirements.

Our data centers meet the highest standards for security and reliability. They are both certified under SSAE 18 SOC 2 Type II standards, which verify that security, availability, processing integrity, confidentiality, and privacy controls are operating effectively. These certifications are validated by independent third-party auditors, providing objective assurance of our security practices.

4. Encryption Standards

All files stored in pCloud are encrypted using 256-bit AES encryption, which represents the current gold standard for data protection. This encryption applies both during transfer (in transit) and while files are stored (at rest). Additionally, pCloud applies TLS/SSL channel protection during data transfer, ensuring that data cannot be intercepted or modified during transmission. The strength of 256-bit AES encryption is such that it would take classical computers millions of years to decrypt files through brute force attacks. This level of encryption is used by governments and financial institutions to protect their most sensitive information, making it appropriate for protecting personal data under GDPR.

pCloud also offers client-side encryption through our pCloud Encryption feature, which provides an additional layer of privacy protection beyond our standard encryption. With client-side encryption, files are encrypted on the user's device before any data is transmitted to pCloud's servers. This approach means that encryption and decryption happen entirely on the user's device. Even if someone gained unauthorized access to pCloud's servers, encrypted files would remain protected because the encryption keys are never stored on our servers.

5. Zero-Knowledge Privacy Policy

pCloud implements a zero-knowledge privacy policy regarding encrypted files. Once a user creates a password for the pCloud Crypto folder, no copies of personal keys or passwords are stored on pCloud's servers. This means that pCloud has no way to access encrypted files, even if requested by law enforcement or other authorities. The zero-knowledge approach provides users with absolute assurance that their encrypted data is private and they maintain complete control over it.

6. Data Redundancy and Disaster Recovery

When files are uploaded to pCloud, they are automatically copied to at least three separate server locations. This redundancy serves multiple purposes. It ensures that user data remains available even if one data center experiences an outage. It protects against data loss due to hardware failures. And it enables rapid recovery in the event of a disaster. Our redundancy approach means that users can rely on pCloud for business continuity.

7. Monitoring and Maintenance

pCloud's infrastructure includes continuous monitoring systems that track the health and performance of our storage systems. Our security teams constantly monitor for unusual activity, potential intrusions, and system anomalies. We also maintain detailed logs of all system access and changes, enabling us to investigate any security incidents and demonstrate our security practices to auditors.

About pCloud

pCloud is a leading cloud storage provider committed to protecting user privacy and data security. Based in Switzerland and operating under some of the world's strictest privacy laws, pCloud provides secure, reliable cloud storage solutions for individuals and organizations worldwide. Our commitment to privacy is reflected in our zero-knowledge architecture, comprehensive security measures, and transparent data governance practices.

For more information, visit www.pCloud.com or contact privacy@pCloud.com.