personal®

SECURITY & PRIVACY PRACTICES

1. Passwords

Only an account owner's password can access a vault and decrypt sensitive data and all files. Personal does not store this password. Instead, passwords are hashed using bcrypt with salting and stretching. As a result, no one - not even Personal employees - can see the sensitive information or any files an owner stores in Personal. If an owner forgets the password and needs to reset it, Personal deletes the sensitive data and all files to protect the owner. We also have mechanisms in place to stop brute force attacks on passwords, and we'll soon offer multi-factor authentication and secure sensitive data recovery.

2. Servers

Data vaults are housed on servers stored in Rackspace, which has 24/7 security guards and biometric security for entry, has been issued an SSAE16 Type II SOC 1 Report, is a PCI Security Standards Council Member, is Safe Harbor Certified, and offers protection via firewalls, its own intrusion detection systems, and other safeguards.

3. Data Storage

All sensitive information and files are encrypted in our servers with 256-bit AES encryption and RSA 2048 asymmetric key encryption. Each container that holds sensitive data is encrypted uniquely, adding an extra layer of security. Non-sensitive information can only be accessed through the user-chosen password that we don't store. While technically possible for a small, limited group of operations employees to access non-sensitive information, they are strictly forbidden from doing so (unless, for example, required by law), and access to our servers is carefully logged.

4. Sensitive v. Non-Sensitive Information

We designate data fields as sensitive (and thus encrypted at rest and not present in a search index) based in large part on U.S. guidelines, including for certain financial, health and other personal data. We go beyond them for data such as usernames/passwords, alarm codes, WiFi codes. All files uploaded to Personal are encrypted, including those stored in linked Dropbox accounts. Non-sensitive data isn't encrypted at rest, which means it can be searched by an owner in his or her vault.

5. Data Transit

We use default 128-bit SSL encryption to protect all owner data, whether sensitive or non-sensitive, and all files while in transit to our servers, meaning from browser to server and when owners access their information or grant access to it to others. Depending on the connection, the SSL encryption can go up to 256 bits. Importantly, we also enable forward secrecy in most browsers and use secure cookies with HTTPS to further protect owner data.

6. Secure Coding and Data Management Practices

We don't use insecure third-party delivery networks, we ensure that user data is never exposed (for example, we use POST rather than GET requests), and we don't see user data even in the context of crash reports. In addition, we don't use data de-duplication methods, which can raise security and privacy concerns.

7. Security Testing and Certificates

We conduct security audits, including penetration testing. We have SSL certificates from GeoTrust and are in the process of acquiring other seals. In addition, we have a number of certified "Ethical Hackers" and "Penetration Testers" on staff who constantly monitor for potential threats and vulnerabilities.

8. Privacy by Design

Personal is the first online, consumer-facing company to be named an Ambassador for the "Privacy by Design" Program by Ontario, Canada Information and Privacy Commissioner Dr. Ann Cavoukian, who coined "privacy by design." This is because our technology and business practices put the user in control.

9. Owners Control Their Data

Only account owners can grant other individuals, companies and apps access to their own vault information, and owners can export and permanently delete it from Personal at any time. We don't allow third parties to track owners in their vaults, and we don't track individuals when they leave our site or native mobile apps.

10. Personal Employees

Our culture makes security and privacy the business of every employee. All Personal employees, from interns to the CEO, undergo rigorous background checks, and everyone, not just our technical teams, receives security training.