

KerberRose Privacy Policy

Privacy Notice

KerberRose believes in protecting our clients' privacy. Please read this policy to understand how KerberRose collects, uses, retains and discloses your personal information.

Types of Nonpublic Personal Information We Collect

Personal information is defined as any data which can be used to identify, locate or contact an individual; including but not limited to: name, email address, mailing address, telephone number, earnings and business information, payment information, etc. KerberRose only collects nonpublic personal information about our clients which is provided to us by our clients or is obtained by us with client authorization.

Disclosure to Third Parties

Personal information is disclosed to third parties only for purposes described in this notice and for which the client has provided implicit or explicit consent.

Employee Training: All KerberRose team members are educated on the importance of keeping personal information secure, both in and out of the office.

Collection and Use of Personal Information

We collect and use your personal information with your consent where we have a legitimate business interest or other legal basis for such collection and use. The personal information you submit to us may be used to manage our relationship with you, including any of your requests, to improve our website or related services offered to you.

We may also use your personal information for marketing purposes, or to send you promotional materials or communications regarding services provided by KerberRose we feel may be of interest to you. We may also contact you to seek feedback on services provided by KerberRose or other research purposes. You may at any time request we discontinue sending you communications, emails or other correspondence by contacting marketing@kerberrose.com.

Any personal information collected by KerberRose is used in the manner outlined in this privacy statement. Your personal information will not be used for other purposes without obtaining your permission, unless otherwise required or permitted by law or professional standards.



Protecting the Confidentiality and Security of Client Information

KerberRose protects personal information against unauthorized access. We make sure to protect and adhere to the following information and procedures:

Client Tax Information: Clients' tax returns containing personal information are secured and restricted to only those individuals with a business reason to have such access. To prevent unauthorized access to tax return information, all electronic files containing this information are password protected. For tax return documentation maintained in hard copy, these files are kept in a secure location where visitors do not have access.

Credit Card Information: We keep all client credit card numbers secure to prevent unauthorized access. Credit Card information is not retained longer than needed.

Transmitting Client Data: When transmitting client data by e-mail using the internet, the e-mail and/or attachments containing client personal information are encrypted and password protected.

When information is sent via facsimile, we verify the recipient fax number and that the fax machine is in a secure location. A cover sheet with the appropriate disclosures regarding IRS Circular 230 is used.

When information is sent by mail, documents are sent by USPS regular mail.

Computer and Cyber Security: All computers are password protected. Each user signs in with a unique ID and password.

For computers connected to the internet, we utilize firewalls, up-to-date anti-virus software, current software security patches and spyware.

We have a wireless access point in each office. These access points are password protected.

We have developed a remote access policy for firm employees. All client data is accessed on firm-issued computers which are protected with robust anti-virus software and two-factor authentication.



Server administrators have a separate and unique ID and password for use when performing system administration activities.

Computer backups with personal information are kept secure and encrypted.

Use and Retention

We limit the use of personal information to the purposes identified in this notice and for which the individual has provided implicit or explicit consent. We retain personal information for only as long as necessary to fulfill the stated purposes.

We adhere to industry-mandated retention periods and either return information to the client or destroy it at the end of this period. Paper information is shredded, and electronic data is made unrecoverable.

Changes to Our Privacy Notice

We may modify or amend any policies in this notice at our discretion. When we do make substantial changes, we will notify you in a timely manner; and any modified or amended privacy policies will be effective for you and your information as of the revision date.