



ADMIN PARTNERS, LLC.

PRIVACY POLICY

This Privacy Notice is effective as of July 31, 2021

This privacy policy is being provided by the ADMIN Partners, LLC. At ADMIN Partners (“we”, “us”, or “our”), we are committed to maintaining your confidence and trust as it relates to the privacy of your information. Please read below and learn how we collect, protect, and use your information.

I: Plan Participant Data

ADMIN Partners, LLC does not sell, or transfer data received from Plan Sponsors to any party outside of the company except where the information needs to be shared with a Plan Participant’s investment provider(s). The information is shared for transaction processing or compliance purposes only.

Data Loss Prevention software is used to detect potential data breaches and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). Monitoring takes place on all web site traffic, email traffic and file transfer traffic. If PII is detected in email communications, the email is automatically encrypted.

ADMIN Partners receives and handles Personal Identifying Information (PII) in one of five ways, described below.

1. Transmission of data from the vendors in each plan is received in standard industry format (Spark Data) under the terms of an Information Sharing Agreement executed with each vendor. Spark Data transmissions are received via a cloud based Secured File Transfer Protocol (SFTP) and stored in a designated network folder. The folder is accessed through the secured network environment by username and password. The data received is immediately loaded into the appropriate administration system for processing. The data is retained in the designated network folder for historical reporting and research purposes.
2. Contribution data files are received through data uploads via cloud based SFTP, or Plan Sponsors can upload data directly to the Relius Administration System (the website address is <https://myplandata.com> and has an active security certificate). These data transmissions are received via Secured File Transfer Protocol (SFTP) and stored in a designated network folder. The folder is accessed through the secured network environment by username and password. The data received is immediately loaded into the appropriate administration system for processing. The data is retained in the designated network folder for historical reporting and research purposes.
3. Email and Fax Transmissions. Data is received directly from Advisors, Plan Vendors or Plan Sponsors via email (service@youradminpartners.com or via fax transmission. The emails or faxes are received and electronically delivered to a secure network folder. The document is then added to our secure document management system and delivered electronically to the responsible processing team.

4. Hard copy requests from Advisors, Plan Vendors or Plan Sponsors received via USPS. These hard copy documents are scanned into our secure document management system and delivered electronically to the responsible processing team. The paper copies are deposited into a locked container and shredded periodically by a reputable third party (Iron Mountain). Should a paper request require holdover to a subsequent business day, the hard copy request is held under lock and key in a designated location.

Data transmitted from Admin Partners to Advisors, Vendors and Plan Sponsors takes place in two ways – as files attached to encrypted emails or as files transmitted through cloud based encrypted Secure File Transmission Protocol.

Data transmitted via email is done through a secured email utility that encrypts the data. In addition, Admin Partners employs Data Loss Protection (DLP) through Microsoft Outlook to identify any PII that may be inadvertently exposed.

Files being transferred via the myplandata.com website are protected via a Secured Socket Layer (SSL) and Data Loss Prevention Software (DLP).

The data held in the Relius Administration System is secured through data encryption at the Oracle Database level. Secured Socket Layers (SSL) are used in web site applications that are used to receive PII. Secured Socket Layers (SSL) employ cryptographic protocols that provide secure communications on the Internet whereby the data is converted from its normal state to unusable data using mathematical algorithms until it reaches its destination and converted back to normal data to be displayed on the user's web browser.

We secure access to all systems through username and password and multifactor authentication for each authorized user. Roles are assigned to each user to control access to authorized segments of the stored data. An audit trail is created for each transaction. The audit trail captures the date, time, username, and transaction details, including type, data elements and confirmation number.

II: Contact and Signup Site Forms

In addition to Plan Data, you may need to provide certain personal information to us when you elect to use certain services available on the Site. These may include: (a) registering for an account on our Site or (b) sending us an email message. We do not collect any personal information about you unless you voluntarily provide it to us.

We use the information we collect about and from you for purposes such as to respond to your questions and requests for services; provide you with access to certain areas and features of the Platforms such as certain products and services; verify your identity; communicate with you about your account and activities on our Platforms; and for purposes disclosed at the time you provide your Personal Information or otherwise with your consent.

ADMIN Partners does not sell your information to any third party.

The same Data Loss Prevention software is used to detect potential data breaches and prevent them. Monitoring takes place on all web site traffic, email traffic and file transfer traffic.

If you wish to modify, verify, correct, or delete any of your Personal Information collected through the Platforms, you may contact us. If you wish to cancel your online account or request that we no longer use your information to provide you services through the platform, contact us at (877) 484-4400 or service@youradminpartners.com.

All data received and processed by ADMIN Partners is maintained for the period required by IRS / DOJ regulations. Data is disposed of in a manner that renders the medium on which it was stored unusable. The destruction of hard drives containing Personal Identifiable Information are certified. The Certificates of Destruction are maintained by the Managed Service Provider and are available on request.

If you have additional questions regarding our Privacy Policy, please contact our Security Officer – Rachel Pastorella by email – rpastorella@youradminpartners.com or by phone at 877-484-4400.