Privacy Statement

Version 1.7 - June 2017

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 only. Personal Identifiable Information (PII) is retained by Admin Partners based on the regulatory standards affecting retirement plans. When appropriate, PII is disposed of in a manner that prevents loss, theft, misuse or unauthorized use of the information

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. ADMIN Partners receives and handles Personal Identifying Information (PII) in one of six 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 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. Information is also sent to Admin Partners via files attached to emails. The incoming emails are encrypted and stored in the appropriate secured network folder for further processing.

3. Contribution data files are received through data uploads via secure network, or a 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.

   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 user name and password 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, user name and transaction details, including type, data elements and confirmation number.

4. Fax Transmissions. Data is received directly from Advisors, Plan Vendors or Plan Sponsors via fax transmission. The 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.

5. 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.

6. Data to Plan Vendors, 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.

Making a Privacy Complaint

If you have a complaint about how we collect, hold, use or disclose your personal information or a privacy related issue such as refusal to provide access or correction, please contact Client Services by email – service@youradminpartners.com or by phone – 877-484-4400. If to make a complaint, the staff member will refer you to a Manager or their delegate and will attempt to resolve the complaint. A response is usually provided to you within 5 business days. We expect our procedures will deal fairly and promptly with your complaint.

If you have additional questions regarding our Privacy Policy, please contact David Scheuring, Senior Vice President by email – dscheuring@youradminpartners.com or by phone – 877-484-4400