Southern Solutions

GDPR Compliance Statement

As part of ongoing support, maintenance, and daily processing, Southern Solutions may record the following data in relation to your company and users directly:

- Passwords
- Remote Connection Information
- Backups
- Network Documentation
- Email Addresses

In order to maintain our GDPR compliance, Southern Solutions ensure all data stored is protected and maintained to high standards, and old data is scrubbed.

Any customers of Southern Solutions have the ability to request their data be scrubbed from our systems. This includes passwords and email addresses of individual employees working for any business we support. Individuals will not be able to request data from replicated backups be scrubbed as this data is stored at a company level, and owned by the customer IT contact directly, not Southern Solutions.

If your relationship with Southern Solutions were to ever end, all data relating to individuals as a whole is not scrubbed automatically, however the option to have your data erased will be given to the signee of the original maintenance contract.

If individuals would like to obtain a list of all current data held about them, they can do so by emailing support@southernsolutions.co.uk and a representative will release all information within 5 business days.

Passwords: In order to carry out automated, scheduled, and reactive works, Southern Solutions keep various passwords stored in an encrypted, fully-compliant, password database hosted in the cloud. As stated, the database is fully GDPR compliant with 256 bit AES encryption, and no passwords are sent or received over email. All devices accessing the passwords must be pre-approved via authentication email and are password protected with complex passwords.

Without the ability to store the majority of passwords kept in the database, daily processing could not take place. In the event that a password is no longer required it is deleted.

Remote Connection Information: To enable fast access to workstations and servers for maintenance and support purposes, we store IP addresses of customer premises within the password database. We also deploy remote access agents to ensure fast access to workstations and monitor select systems for various common issues.

To retain security on this data we ensure it is stored on encrypted systems. We also lock down customer firewalls (where available) to only allow access from the Southern Solutions office via RDP. All passwords for the deployable agent are stored in the encrypted database.

The deployable agent allows Southern Solutions to remotely control user workstations, however to maintain security an option can be set which will either ask the user to accept the connection request before every remote control session, or the Southern Solutions staff member can be

requested to enter a password to gain access. This will never be implemented on servers to allow Southern Solutions to access the server at all times out of hours for maintenance.

Backups/Disaster Recovery: Southern Solutions keep copies of many disaster recovery images for customers on an HA cluster of data storage devices. To ensure that this data is secure the Southern Solutions firewall only allows access to the data from customer sites (authenticated by IP address) and requires a username and password to access. Further to that, all data restorations require a 256 bit AES password to run ensuring that only the customer or Southern Solutions can restore company data.

In the event of information needing to be scrubbed from backups, this can be done but will require the business owner to provide us with permission before we mount and scrub the data.

Network Documentation: Specific customer-related documentation is kept about customers to ensure that effective support can be provided by Southern Solutions employees. This data can include IP addresses and equipment information such as serial numbers and product numbers. It can also include specific processes and procedures around user account and application configuration.

The above information is stored in a password-protected Office 365 backed database and file storage platform to ensure GDPR compliance.

Any data held on these systems is regularly checked for accuracy and can be erased per client request.

Email Addresses: Southern Solutions do not send out marketing emails to customers, nor is a database of companies with no relation to Southern Solutions maintained or used, however it is possible that Southern Solutions may email key account holders with information relevant to security or commonly requested help topics.

When sending out emails to multiple recipients Southern Solutions will either only include staff on the same company in a single email, or multiple recipients are BCC'd into the email to ensure no recipient is aware of any other recipients.

Details of email addresses are also stored on a secure 256 bit encrypted online database if they are supplied by Southern Solutions.

Southern Solutions are committed to ensuring customer data is kept secure and up to date. If you have any questions regarding the data we store about your company please do not hesitate to send a request through to support@southernsolutions.co.uk.