Astute Data Systems Ltd.

Data Privacy Policy

Rev 1.1

Introduction

Astute Data Systems Ltd. are a UK based software development company, with over 35 years' experience of software development, and handling sensitive data.

Under the key definitions laid out under the General Data Protection Regulation (GDPR), Astute Data Systems Ltd. serve the role of 'Data Processor', whereas the users of our software are considered 'Data Controllers', and finally the patient's who's data is held within our software are considered to be the 'Data Subjects'.

Data Storage and Security

Here at Astute Data Systems Ltd, the security of your data has always been our top priority, and while many providers have had to make substantial changes to their infrastructure to meet the new data security requirements outlined within GDPR, we already met these requirements, and in many cases went far and above them several years prior to 25th May 2018.

Any data hosted within our Saas based systems are hosted by RackSpace UK Ltd. who are international market leaders for industry leading secure hosting, and boast an array of ISO certifications for their secure storage infrastructure. All of the data we store with Rackspace is hosted solely within one of their secure London server farms, using dedicated hardware along with top of the line data security measures like a hardware firewall for all incoming connections, as well as IP restrictions, and a ring fenced connection between the public facing app server, and the private database server.

We also implement meticulous security methods outside of the server, like implementing 256 bit SSL encryption to all incoming and outgoing connections, meaning your data is always safe from prying eyes when you use our software, thanks to a high level encryption method used whenever data is saved.

Finally, we also offer and implement a number of security features within our software, like the ‘security groups’ feature which allows managers to restrict the access and privileges they give to their users, or the audit features, allowing users to track changes made within the software.

Data Access and Security

A key aspect of our role is also to support the data controller in using our software, and to do this we're often required to access your database. This access is only ever made at the request of the company, and is only ever made by authorised and trained support personnel.

Access to your database will cease upon the termination of the support request, except in cases where a request needs to be escalated, or revisited. If this is the case, our staff are trained to explain this to the user, giving the user the opportunity to decline this.

To enable the highest level of security, support staff are only authorised to access a customer's database while located within our offices, and upon the termination of any staff member employed by Astute Data Systems Ltd. all credentials for gaining access are updated in such a way as to remove any means to the former staff member gaining access to this data.

In some extreme circumstances, errors may occur within the user's system that require escalation to our senior development team. In these cases, they may need to download a copy of the user's database so that they can troubleshoot the error without the risk of corrupting or altering any live data. Should this be required, the staff member handling the request will explain this procedure to the customer, again giving them the ability to decline this measure of escalation. The support staff will also then track the progress of the fault escalation, ensuring only the required data is downloaded, that the download is managed in a secure and compliant manner, and finally that the duplicate database is promptly destroyed upon completion of the task.

In cases where we are required to download a user's data, we will do so via a secure, encrypted data transfer method, and we implement strict policies on the storage, and eventual destruction of this data.

Due to the extent of data we are able to access upon the request of the data controller, and that often multiple employees of the data controller could contact us for support, it is extremely important that due diligence is taken on both parties part.

Data Transfer & Email Security

While every effort is made to secure the safety of the data while it is stored on our servers, there are cases in which the data can be transferred outside of our system i.e. during the data transfer involved in accessing the software, or when sending emails.

When a user logs into the software, either via the App, online booking portal, or desktop system, a dedicated connection is made to one of our dedicated Application servers - these servers solely house the software, and no data. A ring fenced connection is then made from the Application Server to the Data Server, meaning no connections can be made to the databases from any other device.

When any data is sent to or from the client to the Application Server, these connections use 258-bit end-to-end SSL encryption to ensure the maximum level of data security.

In cases where an email is sent from the software to a third party i.e the patient, these emails can go in one of two ways:

Via our own Mail server - These emails use the same high level encryption as the other data transfers from the system. We normally use our own mail server for the more system critical emails like appointment reminders, and confirmations.

Via SMTP - For Recalls and mail-outs, we require the system user to enter their SMTP details in the general setup area - when doing so the user will have the ability to enable encryption, should their chosen mail provider support this.

Third Party Processors

We offer a number of third party integrations within our products, enabling users to expand the functionality of the software by incorporating third party functionality. We refer to these simply as ‘integrations’.

We currently integrate with the following third parties:

- **PCA Predict;**
  PCA Predict are a Royal Mail postcode lookup service, who offer a premium service, allowing users to search for address’ by a postcode, saving them time in completing basic contact detail entry. Users can opt into this integration by entering their API key (Which is provided by PCA predict when commencing a contract with them) into the ‘integrations’ area of our software.
- **Intelli SMS;**
  Intelli SMS are our chosen operator for managing all SMS messages that go out through our software. Users can opt into using the SMS service by ticking the ‘Enable SMS’ option in general setup.
- **HealthCode;**
  Healthcode offer an insurance billing service for healthcare professionals, allowing them to digitally generate invoices for insurance patients. Users can enable the Healthcode Integration by completing the setup steps within the Integrations area of setup.
- **Mailchimp;**
  Mailchimp offer automated Email marketing tools for running mail shots, and managing subscription lists. Users can enable this feature by entering their Mailchimp API key in the integrations area of setup.
- **PhysioTec;**
  Physiotec offer a Physio exercise tool, allowing practitioners so send exercise guidance to their patients, pulling basic patient data from PracticePal. Users can enable this by entering their API key in the Integrations area of setup, then enabling it on the relevant users’ accounts.
- **Stripe;**
  Stripe are a payment gateway, and are our chosen payment solution for our online booking platform. Users can enable this by entering their API key in the Integrations area of setup
- **Google Drive;**
  We have not yet released our API with Google Drive, but we will update our documentation to reflect this fully when we release a supported version of this.

All integrations are offered as an optional service, meaning users are not required to use any of these services to use the basic functionality of our software. Before integrating with any third party platform, we carry out the required due diligence tests, as well as auditing the data

transfers required to facilitate an integration, putting together the relevant documentation, and risk assessments.

The Data Controller is also obligated to carry out their own due diligence tests on any third party platform, before opting into its usage.

What We Collect

While we do host the product, and manage the storage solutions for the data handled by the products, we do not handle or collect any of the data you enter within the software. We do however collect certain data on the software licence holders.

The reason we hold this data is because we require this data to provide the software to our users. We currently collect and store the following data for our licensees:

- Primary Contact Name
- Business Name
- Business/ Primary Contact Address
- Primary Contact Number/s
- Primary Contact Email Address
- Billing Email Address
- Date of initial contact
- Date of receipt of documentation and direct debit
- Date of Contract inception
- Billing and payment history
- Basic usage statistics*

*We currently only record the data of an account's last login, the total number of patients entered into the system, and the total number of bookings entered into the system. These are collected and stored as a single numeric value, and we do not collect any more specific data than this. We record this data to ensure accounts are not left dormant while a contract, or trial period is still live.

All of this data is held on a secure, dedicated system that meets the same security standards as outlined in the 'Data storage and security' section of this document.

Astute Data Systems Ltd has appointed the BACS Approved Direct Debit Bureau, Eazy Collect Services Limited (www.eazycollect.co.uk), to collect your payments and to securely store the information provided on your direct debit mandate. Eazy Collect Services Limited is a PCI compliant software vendor. We are however required by BACS to securely store your original mandate.

In cases where a customer is based outside of the UK, and as such, is unable to provide UK based bank details, we are unable to set up a direct debit and instead take details of a nominated credit card. These details are held in an encrypted database, and are only accessible for billing purposes.

Policy Reviews and Revisions

We will endeavour to review, and where required, update our documentation on an annual basis. We reserve the right to update this policy, without prior warning or written consent, at any time.

The most recent version of this document will always be made available via our website, or on request.

Contacting Us

Should you have any questions regarding this document, please contact our dedicated support team via info@practicepal.co.uk.

Should you have any questions in relation to GDPR, please contact our designated Data Protection Officer via thom@practicepal.co.uk