Data Handling

Introduction

PAS Ltd have a data handling policy because the data is the most important part of a computer system. It's the most important part of a computer for our customers and it's the most important part to us.

Data security means the data is not liable to loss from hardware failure, hardware theft and protected from unwanted viewing.

As part of our normal routine we could collect and store customer data in several ways - in all cases data that we work with should be anonymised before being transferred to PAS Ltd. The P11D Organiser has in-built routines to anonymise data, replacing all personally identifiable content with random characters - transactional integrity is maintained using internal references, but the ability to identify individuals is removed.

- We collect and store anonymised customer data to investigate problems experienced during the use of one of the software packages we supply.
- We store customer anonymised data on our own computers whilst it is being investigated and /or repaired.
- We store anonymised customer data on various storage devices (USB sticks, CD/DVD, hard disk drives to name a few) as well as several secure online data storage facilities.

Our experience of data security

Our experience of handling data securely is extensive, and we have handled data for thousands of businesses over our 20+ years of trading. We have handled data for large companies where the sensitivity of the data is of paramount concern. We have also handled data for companies who deal with personally identifiable information. Therefore, data security is an extremely important issue for us.

Storing customer data

Customer data usually arrives with us in one of the following ways: -

- Customers transmit the anonymised data to us via a secure HTTPS connection to our ISO27001 data centre. The data (even in anonymised format)is unreadable unless it is restored to the same software package.
- Occasionally one of our technicians will connect to a customer PC or server using a secure, encrypted remote connection service such as GoToAssist. This encrypted service is the most secure way of accessing a customer device (and our preferred method) to obtain a copy of the anonymised data for investigation and repair purposes.
- As a last resort anonymised data can be sent to us on physical storage medium such as USB stick, CD, DVD, USB hard drive, PC hard drive or similar - this is not recommended.

The data should ideally have backup copies made and be secured by the customer, before it is sent to us, to their own satisfaction.

Upon receipt, customer data is moved to a secure area of our computer network to which only support technicians have access. All servers and computers on our network are secured with password protection and are behind a firewall to prevent intrusion from outside the company and from any other computer connected to our network.

The transactional data is not encrypted (although the key data is anonymised) as this can make repairing the data more difficult.

After the repair has been completed the data is deleted from our computers within 1 week of the completion of the repair. Periodically the free space on our computers is wiped.

The data will also be scanned for viruses, spyware and any other kind of malware for ours and the customer's protection.

During a repair of data we may use a third computer or storage medium to facilitate this. Our copy of the customer data is immediately deleted and wiped in the periodic free space wipes.

Limitations

To manage customer expectations we must point out the limitations of our storage of data:

- Nothing we do to secure customer data constitutes a backup solution for use by our customers.
- Some storage devices occasionally come to us in a less than reliable state. This means your data may already be at risk. We will endeavour to retain the data but you are ultimately responsible for your data and if you do not have a sufficient backup solution in place before your computer fails there may be nothing we can do and we do not accept any liability for the loss of data in this situation.
- We can advise you on the best approaches to take to backup of your critical data – please contact us to discuss this in more detail.
- We have liability insurance but where hardware can easily be replaced, data cannot.

Hosted (SaaS) Data

Where PAS Ltd has control of your data (for example, you are using our hosted provision) we will maintain working copies and backups all the time a customer is licenced to use the software. If a customer decides to terminate their contract, our standard policy is to retain the data for a 'cooling off period' or until the end of the then current tax year. This allows for a decision reversal and ensures the customer can remain compliant with HMRC reporting. On termination, should the customer decide they want you data deleted with immediate effect, they should send a written request to support@p11dorganiser.co.uk.