Property & Funding Solutions Ltd
Registered Office: 6th Floor, 60 Gracechurch Street, London EC3V 0HR

PERSONAL DATA SECURITY POLICY

Personal Data:
Any information relating to an identifiable person (living individual), who can be directly or indirectly identified by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including but not limited to name, address, date of birth, identification number data or online identifier.

Sensitive Personal Data:
The General Data Protection Regulation (GDPR) refers to sensitive personal data as 'special categories of personal data'.

The special categories include data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health or a natural person's sex life or sexual orientation.

Property & Funding Solutions Ltd (PFS) holds personal data and recognises that this could be a high value commodity for fraudsters.

In line with Principle 2 (skill care and diligence – a firm must conduct its business with due skill, care and diligence) and Principle 3 (management and control – a firm must take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems) of the FCA's principles for business and in accordance with Principle 6 of the Data Protection Bill (personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data. The risks referred to include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data) it is PFS's responsibility to secure customer data.

PFS has assessed the financial crime risks associated with its customers' data. The business undertakes a Data Security Gap Analysis annually and any agreed improvements have a business owner and delivery date allocated to each enhancement and ongoing monitoring is undertaken until the enhancement is delivered.

PFS has put in place systems and controls to counter the risk that the business might be used to further financial crime.

Where business projects involve the collection, use, storing and processing of personal data PFS complete a Privacy Impact Assessment to manage the security of that data.

As a business we adhere to the requirements of GDPR and are registered on the Information Commissioner's Office (ICO) Data Protection Register. This can be checked by visiting https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Responsibility:

PFS takes Personal Data security seriously and has given its Managing Director overall responsibility for the business's approach to Personal Data security. This does not diminish each employee's responsibility to ensure that customer data in their possession is kept secure at all times. Training is provided to ensure that employees understand their responsibilities and the ultimate risks of a breach of customer data security.

PFS recognises that customer data security issues permeate the whole business and it is not restricted to an IT issue.

Security:

PFS ensures its business premises are secured when unoccupied and access to the premises is continually monitored with all employees and visitors signing in and out. The business has in place physical security to minimise the risk of data theft and/or a break in.

Visitors are not left unattended with access to Personal Data even when the business is confident of the visitor's integrity.

Recruitment:

PFS is confident that its employees have the integrity to handle Personal Data. The business undertakes appropriate checks at the point of recruitment and if anything comes to light that questions an employee's integrity the matter is sensitively and promptly reviewed.

Individual Responsibilities:

As a business:

- we do not leave Personal Data on desks unattended
- we adhere to a clear desk policy
- we ensure that Personal Data is not shared unnecessarily
- employees are required to sign and abide by our confidentiality agreement
- we encourage our employees to raise concerns about customer data security with the Data Protection Responsible Person however insignificant they feel them to be
- we only collect the personal information that is needed for a particular business purpose
- records are updated promptly if information changes (e.g. a change of address).
- Personal Data is disposed of in accordance with the firm's Data Retention Policy and in accordance with GDPR once it is no longer required
- we carry out identity checks before releasing personal information to someone over the telephone

Education and Training:

Training on GDPR is ongoing as PFS recognises the quickly evolving nature of financial and internet crime and the need to ensure that employees' awareness on these topics is maintained.

As part of the induction process employees are advised of the importance and relevance of customer data security and are provided with a copy of this Policy.

All employees sign to acknowledge that they have read and understood PFS's Personal Data Security Policy.

IT:

PFS ensures that each employee has their own user name and password. Employees are instructed not to write passwords down or share them with colleagues. As a business we are aware of the importance of strong passwords and the importance of changing passwords regularly.

Employees are advised that passwords must be at least seven characters in length and contain a mix of upper & lower case letters, numbers and symbols.

Employees lock or log off from unattended computer terminals. Any portable IT equipment issued to an employee is their responsibility and they must do their utmost to keep it safe.

PFS does not permit Sensitive Personal Data to be removed from the premises unless essential.

Employees who work remotely are able to connect to the network and therefore customer data is not held on lap tops, memory sticks or CDs.

The IT systems are backed up daily and the data held securely off site. Data is encrypted.

Any concerns regarding IT and customer data security should be raised immediately with Property & Funding Solutions Ltd at 27 Phipp Street, London EC2A 4NP (F.A.O: Managing Director).

Customer data that is removed from the premises is encrypted if it would cause damage or distress if lost or stolen.

To minimise the likelihood of PFS's IT system being hacked into or being affected by a virus, the IT department has installed security software and the firm ensures that this is upgraded regularly.

Disposal of Data:

The firm disposes of Data appropriately depending on its nature / sensitivity.

Our policy is to shred sensitive personal data.

PFS encourages any concerns that customer data is not being disposed of appropriately to be raised.

Data Security Breach Management:

In the event that customer data security is lost or stolen, the matter is to be reported immediately to the Data Protection Responsible Person who will:-

- Contain the security breach and recover data where possible
- Assess the ongoing risk
- Notify the persons concerned including the appropriate regulatory body
- Evaluate the breach and the effectiveness of the firm's response to it
- Carry out root cause analysis and review lessons learnt in order to implement any necessary enhancements to seek to mitigate the risk of the data security breach being repeated