Smoke Hall
Smokehall Lane
Winsford
Northwich
CW7 3BE
0161 989 5908

Data Protection Policy

The purpose of this document is to detail the firm's policy and procedures for data security and protection. The policy applies to all data processed by the firm, both digital and in hard copy and to all staff employed by the firm including temporary staff and contractors. The policy is designed to ensure compliance with GDPR, Data Protection Act 2018, PECR, FCA rules relevant to recording, processing and retention of personal data and all other relevant legislation and regulation.

The firm has a separate Privacy Policy Statement that details the reasons why customer's personal data is obtained, its sources, how it will be processed and customers' rights. The privacy policy is required to be made available to all customers and stakeholders on the firm's website and on request.

Lawful basis for processing

Customers' personal data will only be processed where there is a lawful basis for doing so. In most cases the basis will be consent. Consent is required to be freely given, informed and the consent given to process the customer data for the specified purpose unambiguously stated. Consent cannot be inferred through a failure to uncheck a pre-ticked box. Customers must be clearly informed that they can withdraw consent at any time and provided with a simple cost free means for doing so.
In some circumstances legitimate interest may be used as a lawful basis for processing customer data. Details of the circumstances for which this may be used are contained in the firm's Privacy Policy. Legitimate interest must not be used as a basis for processing data until the firm's compliance oversight manager has conducted a formal legitimate interest assessment, this must be in writing and stored for reference and in the event of any requirement to be disclosed to a regulator. Use of legitimate interest as a basis for processing will only be authorised if, following assessment, it is considered that customers would have reasonable expectation that their data might be processed in this way. Customers are required to be able to object to the processing of their data on this basis and where they do so processing of that customer's data must cease.
Our policy when processing personal data is to obtain the least amount of identifiable data necessary for the purpose required.

Data Sharing

There may be circumstances where customer data is obtained for the purpose of referral to a business partner who will offer to assist in the processing of the customer's prospective claim. This service requires data to be shared with claims processing businesses to whom the customer's prospective claim is intended to be referred. Customer data will only be shared on this basis following obtaining the customers informed consent to do so.

In all cases a data sharing agreement is required with the party with whom data is to be shared. The agreement is required to state the purpose for which the data is being shared and that the sharing party may not process the data for any other purpose. Data transfer will be restricted to the data that is reasonably required to perform the service. The agreement is required to stipulate that the data sharer's sub-processors and all of their personnel will, at all times, comply with all data protection legislation in connection with the processing of the data and the provision of the services and will not, by any act or omission, cause the firm (or any other person) to be in breach of any of the data protection legislation. The agreement must also require that the receiving party has implemented appropriate technical and organisation control measures to ensure the security of processing.

All data will be exchanged through a pre agreed transfer protocol, which in all cases will require the use of a secure API link to receive the transfer. Data may be shared with third party bodies such as regulators without customer consent but only where the firm is under a legal obligation to do so. Customers are informed of the circumstances under which their data may be shared in the firm's Privacy Policy.

Data Retention and Destruction

It is the firm's policy to keep customer records which will include personal information for a minimum period of 6 years and maximum of 7 years from the latest of:

- The customer withdrawing or deciding not to pursue the claim;
- The settlement of the claim;
- The conclusion of any legal proceedings commenced in connection with the claim;
- The conclusion of the handling of any complaint made by the customer to or about the firm, including the handling of the complaint by an alternative dispute resolution scheme (such as the Financial Ombudsman Service);
- The termination of the agreement between the firm and the customer;
- The date of the firm's last contact (by whatever method) with the customer.

The reason for the decision to retain customer data for a minimum period of 6 years is that the firm is FCA regulated and subject to Financial Ombudsman Service jurisdiction. The limitation period for a customer to make a complaint under Ombudsman rules is 6 years from the date when the issue that is the subject of the complaint occurred. Customer data is therefore required to be retained for this period in order to ensure that any complaint received inside the limitation period can be fully investigated and dealt with fairly.

It is the firm's policy to retain staff records for minimum period of six years and maximum of 7 years from termination of employment with the

Smoke Hall
Smokehall Lane
Winsford
Northwich
CW7 3BE
0161 989 5908

firm. This will include records relating to any disciplinary investigations and actions taken against a member of staff during their employment. The reason for this retention period is that the firm's regulator requires the firm to provide any other FCA regulated firm considering employing a former member of staff with a reference which is required to detail any disciplinary actions taken against the member of staff in the previous 6 years.
It is the firm's policy to carry out an audit of records held annually in January of each calendar year. All personal data relating to customers and former members of staff that have been held for longer than minimum retention period will be deleted from both primary and backup systems following the conclusion of the annual audit.

Data Security

In order to ensure high levels of data security within the firm, Lee Robinson, the consultant employed to provide IT support to the firm, has been designated person responsible for data security supervision. The role requires him to provide technical advice with regard to security issues to ensure that the firm's data security policies are robust and in accordance with best practice with regard to the nature and size of the firm.
We have stringent safeguards to protect client data from theft. All client data is kept solely on two cloud-based data bases which are updated in real time, client data is not stored on site. The data bases have an inbuilt firewall and anti-virus software. The system requires a username and password to access, with the additional encryption safety feature via 18 key stroke auto backup passwords, automatically generated by the system. The system locks down access to the databases to specified IP addresses so that it cannot be accessed from computer equipment other than that owned by the firm. To change an IP address requires a request to the database administrators, who will only do so if requested by designated senior managers.

Use of Computer Equipment Protocol

In order to control the use of the company's computer equipment and reduce the risk of security threats the following will apply:-
Only IT equipment supplied by the firm may be used for business purposes. This includes where staff are working off site.
Only authorised staff may have access to the company's computer equipment.
Computers should be locked and put in sleep mode when staff are away from desks including when working off site.
Staff are prohibited from connecting any portable storage device to any of the firm's computer equipment without first obtaining the approval of the director and arranging for the IT department to scan the device to ensure it is virus free.
Only software that has been authorised by the firm for business applications may be used on any of the company's computer equipment. All new software must be authorised by the director and virus checked by IT before being used.
The office is paper free. Any post received from customers is required to be scanned to the customer record on the CRM system and then placed in confidential waste or returned to the sender. All confidential hard copy waste is required to be placed in confidential waste bins to be removed by an authorised service provider for shredding.
Office phones can only be used for work related purposes. No work related phone communications should be carried out on any other devices to ensure all calls are recorded.
Staff computers, telephones and email accounts are required to be password protected. Staff are required to update their passwords every 90 days using the firm's password protocol:

- Passwords are required to be a minimum of 12 characters.
- They require to contain at least one number, one special character, one upper and one lower case letter.
- Passwords are required to be unique and not be used on any other device or system.
- Staff must not reveal their passwords to anyone.

Email Protocol

The E-mail system may only be used for communications and matters directly concerned with the legitimate business of the company.
Staff are advised that email phishing is the most common cause of cybercrime.
Staff are required to be vigilant with regard to suspicious incoming emails. They are instructed not to open any email attachments unless they are aware of the identity of the sender and the nature of the content of the attachment. They are advised not to respond to any email where the sender is unknown and on no account even where the sender is known disclose passwords or any other security sensitive data in any email response. If a member of staff is unsure how to proceed they are required to obtain advice from IT before taking any action with regard to the subject email. All spam and suspicious emails should be deleted.
Staff are required to take care with the content of emails, proof reading carefully before sending. In particular double checking the email address of intended recipients including any that are copied or blind copied.
If a member of staff inadvertently sends an email to someone other than the intended recipient they should immediately attempt to retrieve it. If they are unable to do so they must straightaway email the person to whom the email was sent to by mistake, informing them the email was sent in error, requesting they delete it and to confirm they have done so. Having undertaken this action and in any event within one hour of becoming aware of the data breach the Compliance Oversight Manager or in their absence the firm's director must be informed. They will advise on next actions which will normally be to provide them with a copy of any data disclosed in and attached to the email in order they can assess the seriousness of the breach and direct any required action.

Internet Use Protocol

The internet system is available to staff for legitimate business use and matters concerned directly with their employment. Staff are prohibited from

Smoke Hall
Smokehall Lane
Winsford
Northwich
CW7 3BE
0161 989 5908

accessing the internet from the firm's IT equipment for non-work related activities.
The firm utilises the router and a firewall to restrict internet use by blocking websites that are not white labelled for work use.
Staff are required to obtain IT approval before downloading material from internet sites.
All staff employment contracts reserve the right to monitor all E-mail/Internet activity on the firm's IT equipment for the purposes of ensuring compliance with their policies and procedures.

Social Networking Sites

Staff are prohibited from posting any work related issue or material on any such site at any time either during or outside of working hours and includes access via any computer equipment, mobile phone or PDA.

Data Breach Protocol

A data breach is defined as where any personal data that the firm is responsible for has been lost, accidentally destroyed, altered without proper permission, damaged or disclosed to someone it shouldn't have been. Where a data breach is identified this must be reported to the firm's Compliance Oversight Manager (COM) or, in his absence, the firm's director. The report must be made within 1 hour of becoming aware of the breach.

The COM will urgently gather and correlate all available information relating to the breach and assess the seriousness. First step will be to consider and direct any actions to be taken to mitigate potential harm/impact of the breach.

In carrying out the assessment he will consider the number of persons likely to have been impacted by the breach and the potential severity of risk and/or harm to those whose personal data may have been wrongly lost or disclosed. Having considered all available information a decision shall be taken whether the person(s) whose data may have been disclosed or lost should be informed and whether the breach is of a nature that requires a report to be made to the ICO. In the event that a decision is made to inform the affected persons and/or report the breach, this requires to be done as a matter of urgency and in any event within 72 hours of becoming aware of the breach. Where the breach is considered to be reportable the FCA must also be informed.

Whether or not reportable any breach must be recorded in the firm's Data Breach Register, providing details of the reasons in the event that the persons affected by the breach were not informed and/or that the breach was not reported.
Whether reported or not root cause analysis is required to conducted with regard to every breach, causes identified and actions recommended in order to avoid recurrence.

Compliance and Monitoring

Due to the firm's size, it has been determined that the firm is not required to have a Data Protection Officer, as it does not process special categories of data on a large scale. However, in order to provide oversight of compliance with this policy and ensure it is regularly reviewed and updated to reflect any changes in data protection legislation, regulation and best practise our Compliance Oversight Manager has been allocated many of the tasks required to be undertaken by a DPO.

With respect to Data Protection the Compliance Oversight Managers key responsibilities are:

- To keep himself updated with regard to data related laws, regulations and guidance, and to report on such to the firm's director advising on any necessary changes to this policy and to any other relevant policies and procedures.
- Overseeing changes to processes;
- Monitoring oversight to ensure compliance with this policy, the GDPR and the Data Protection Act 2018, PECR and any other relevant legislation and regulations;
- Providing a summary of the firm's data protection compliance performance as a standing item in the quarterly Compliance Report for distribution to the director and any other relevant members of staff.
- Review this policy annually and advise/recommend any changes for implementation by the director.
- Act as point of contact with the ICO and FCA with regard to data protection issues.
- Assessing data protection breach and ensuring prompt reporting to ICO and/or FCA of reportable breaches.
- Where any data breach is identified or any issues relating to non-compliance with this policy, to conduct root cause analysis to identify any underlying causes as to why the issue occurred and advise the Director of interventions required to avoid recurrence.
- Ensuring all staff receive data protection policy training on induction and annual refresher training. Also to devise and deliver training to all managers and staff in the event of any significant amendments to this policy.

(January 2024)