FinCalc

Company Policies

FinCalc

c/o O&M Pensions Solutions
5 Kings Court, Newcomen Way,
Colchester
Essex, CO4 9RA

02/24

Tel. 01206 803210
Email. sales@fincalc.co.uk

CONTENTS

ABOUT US

COMPANY NAME	O&M Pension Solutions Ltd
TYPE OF LEGAL ENTITY	Limited Company
OFFICE ADDRESS	5 Kings Court, Newcomen Way, Colchester, CO4 9RA
ESTABLISHED	December 2013
EMPLOYEE COUNT	18

O&M Pension Solutions are a developer and provider of financial planning software and services. Our solutions are used by members of the financial services industry such as advisers, paraplanners and product providers.

DATA PROTECTION

We understand the importance of protecting not only your personal data but that of your clients as well. As per our software licence terms all information that we process and/or control is done so in line with the UK GDPR. For clarity we may process and/or control the following information:

Your personal data

- Full name, business email address, business mailing address, contact telephone number, business Bank Account details.

Your client's personal data

- This is data that is shared with us within our software application.
- Can include title, name, date of birth, marital status, spouse's date of birth, address, national insurance number, pension scheme reference number, salary, pension values and other financial data.

We will allow our customers to conduct audits and inspections in order to verify our compliance with relevant data protection legislation.

Data transfers

All personal data relating to your clients, including backups, is held exclusively in the FinCalc platform hosted on UK based Microsoft Azure data centres. No data relating to your client's is held on the file servers located at O&M's offices, nor transferred outside the EU.

We may transfer your personal data outside of the EU. This is strictly limited to contacts who use our software as we use Xero for accounting purposes. See Sub-Processor section for further details.

Data transfer safeguards

Using Office 365 for all email communications, we have data loss prevention policies in place that capture:

- Any bulk export of information.
- Any emails that are sent outside of the organisation are limited by file size.
- If the recipients' domain is located outside of the EEA these emails are monitored.
- Personal webmail services are blocked.

Access to the Azure database, which is where your client's personal data is stored, is strictly limited to Director and Senior Management level only. All access to the Azure Database is recorded including the data that has been accessed and the reason for access. We will not amend any customer client data.

Notification of data processing/control changes

For detailed information about the way we process your data please view our Privacy Information Notice (PIN). The link to this document is also available on our outgoing emails. If our data processing and/or control procedures require any amendments, we will contact you in advance by written instrument.

Sub-Processors

Details of our sub-processors are below: -

Microsoft

All client personal data that is processed by us is stored on secure UK based Azure data centres. We use the following services to process your data:

- Office 365 – Business emails including those which may display and/or have as an attachment, client's personal data.
- CRM – Your business contact information as previously specified is controlled by us on this platform.
- Azure – Your personal data and your client personal data.

Xero Accounting Software

Used for accounting purposes including invoicing our customers and storing licence agreements.

Any personal data that is transferred to Xero is limited to First Name, Surname, Email address and Company name. Bank Account details are not stored on this software.

We have ensured that they have appropriate safeguards in place. Please see their Privacy Notice for further information.

JumpCloud (DAAS)

JumpCloud are a cloud-based directory as a service provider. It enables us to manage access to our systems and links to our Office 365 account. Further information on JumpCloud security can be found here.

Datashredders

All paper files received by us are securely destroyed onsite by Datashredders Ltd within 3 months of finalising the work required. Datashredders also provide us with secure disposal of all electronic devices and hold the following accreditation – *Information Destruction BS EN 15713:2009*.

Please visit their website for additional information.

GoCardless

We use GoCardless to process our direct debits. Any new direct debits are set up using GoCardless. You can view their privacy policy here with details of information that they may collect from you.

Any data input is stored within the EEA.

DocuSign

Any legal documentation is sent via DocuSign. As this company is based in the US, we have ensured that they have appropriate safeguards in place for all personal data that is shared with them. You can view their privacy policy here.

They also have a binding corporate rules policy which you can find here.

Should we alter, or require additional, Sub-Processors we will notify you of any new appointments made where this would impact existing customers. We do not foresee any changes or additional sub-processors being required and any changes to sub-processors would be vital for the performance of the service.

Any new sub-processors would be appropriately reviewed to ensure that any data we process with them would be within the UK/EU or, if there were no alternatives, would provide appropriate safeguards.

Duty of confidentiality

All staff have a duty of confidentiality and have agreed to this as part of their contract of employment.

Where a sub-contractor is appointed, at no point will they have access to your data.

Any staff or sub-contractors would be subject to the same duty of confidentiality when they are contracted by the company.

We provide annual data protection and cyber security training to staff to ensure their knowledge is up to date and issue updates throughout the year when there are any policy changes.

Data subject access requests (SAR)

Requests from your clients

Should we receive a request from an individual they will be asked to complete and return a SAR form. Upon return of the form we should be aware of which customer the SAR relates to. We will then contact our customer to make them aware of the SAR prior to any information being released to the individual.

If we cannot identify which customer the SAR relates to we will conduct a search of our database for the individual concerned. We will then conduct additional searches in order to determine which customer the request is related to, following the same procedure as stated above once the customer has been identified.

Requests from you

We can provide copies of your personal data that we store upon receipt of a written request.

Personal data breaches

In the event of any personal data breach our internal Data Protection Team will investigate and report to the impacted parties within 48 hours of it being identified. We will provide details of what information was affected, how it happened, and any steps taken to mitigate future risk. Additionally, we will inform the supervisory authority (ICO) within 72 hours of the breach being identified. A copy of our Breach Reporting Procedure can be downloaded here.

INFORMATION SECURITY

Software Controls

The software and applications that we use have built-in security features. The following explains how we utilise them:

Microsoft CRM

Our customer management system which is used to store your personal data along with the details of the products and/or service that you subscribe to. Access to CRM is limited only to staff who require it. Additionally, Microsoft CRM provides additional security roles which restrict functionality depending on the individual user requirements. These are reviewed regularly to ensure the security roles are assigned appropriately.

Microsoft Office 365

All staff have access to core apps such as Word, Excel, Outlook and PowerPoint. We also utilise SharePoint groups as a means of sharing internal documents and access is restricted to members of these groups.

Additionally, we utilise multi factor authentication so that if a member of staff is looking to access any of these apps using a new device they are required to successfully complete this process.

JumpCloud (DAAS)

Is used to manage and monitor individual staff systems, such as allowing or blocking access to specific company hardware. We also use JumpCloud to enforce our PC security policies as outlined under Internal Security Policies.

JumpCloud also drives our password policy for user access to their PC, network drives and Office 365. The rules we set for password protocol are as follows:

- Minimum character length.
- Character specific requirements – lowercase, uppercase, numeric, special.
- Password cannot contain a Username.
- Password cannot match any of the last 5 used.
- Password expires every 90 days.

Xero Accounting Software, DocuSign and GoCardless

Access is limited to a small number of staff who require it. Multi-factor authentication password protocol is activated within the software to provide additional login security where available.

ESET Endpoint Security

All PC’s within the office have ESET installed, this is secured by cloud policies enforced on each individual PC with user access unable to make changes. This is a subscription based application and all necessary updates are applied automatically.

Office Controls

In addition to the aforementioned Software Controls, we also utilise a range of internal office controls to further mitigate security risks.

Software Inventory Management

A list of all software applications that our staff access to assist with their regular duties is kept and updated regularly.

Cyber Essentials Plus

We are a Cyber Essential Plus accredited company, our certificate is available to view on our due diligence page along with the National Cyber Security register. This is renewed annually.

Office Based Servers

These house drives which hold general information available to all staff and departmental information which is only available to those who require access.

Remote and physical access to the servers are limited to key senior staff members only. The servers are situated in our office.

Our local servers are backed up using Microsoft Azure.

Staff Security Protocols

Our staff are fully aware of the importance of internal security protocols that we expect them to follow. These protocols are documented and cover the following:

- Clear Desk Policy.
- Secure storage and disposal of paper records.
- Visitor access controls.
- Email security awareness.
- PC security policies such as locking screen when away from desk, end of day shutdown, cannot connect external instruments via USB or CD.
- Telephone security awareness.
- Ongoing monitoring to ensure staff compliance with the above.

The policies above are reviewed periodically to ensure continued compliance. Should we be aware of any member of staff being non-compliant with any staff security protocols, further training may be provided and/or disciplinary action will be taken.

Employees

We use external recruitment agencies to source new staff when required. They complete their own checks on potential candidates before referring them to us. We also conduct the following checks on new employees:

- DBS checks
- Identity confirmation (passport etc)

All new employees are presented with a formal contract within which they agree to a Code of Ethics, Acceptable Use Policy and a Non-Disclosure Agreement.

We provide data protection and cyber security training to all members of staff to reinforce their knowledge and understanding of current legislation.

As far as possible we ensure that all critical duties are segregated between staff, other than at Director level.

Access Control

We maintain an access control register to ensure our users only have access to software and services that are relevant to their role. This is reviewed annually or sooner if a user changes role.

For privileged roles, these are reviewed more regularly to ensure that these also remain relevant to the employee and their role.

For any leavers, access to all software, systems and apps are terminated on their final day of working.

General Office Security Procedures

Our office is a privately rented self-contained space. The building's landlord provides 24-hour security cover. There is one main access door to the building, secured by a key lock. The building is alarmed out of office hours.

Visitors to our office are only able to gain entry via the front door. Upon entry to our office space we request all visitors sign into our guestbook at which point a Visitor Pass is issued to them. Upon leaving all guests must return the Visitor Pass to us and sign out using the guestbook.

Any unknown visitors are challenged by staff members.

FinCalc Web Application Security

To ensure our software is safe and secure for our customers, we have a range of controls and tests in place.

Customer Controls

As a software firm we understand the need for our customers to have access control over their use of our application. Therefore, our application provides a range of inbuilt security features which can be customised to suit company requirements. We have a Security Guide document which explains these feature that all users can download via the application.

Penetration Testing

Our application has undergone a rigorous penetration testing process. You can view our Attestation Report on our due diligence page.

Penetration Tests will be undertaken every 12 months to ensure compliance with our accreditation.

Development and Maintenance

All software development is carried out internally, we do not use 3rd parties during this phase. Rigorous testing procedures are in place to ensure accuracy in terms of software calculations. These are conducted during development and prior to any update being deployed. Further tests are also undertaken at regular intervals. Records of software updates and ongoing developments are kept ensuring we have an audit history of any changes that we have made. Tests are conducted in a separate environment to production with both environments benefitting from identical security measures. Dynamic application security testing is carried out on both the live and production environments.

BUSINESS CONTINUITY

The majority of our software and services operations are cloud based, meaning there would be minimal disruption to what we provide should we be impacted by any unforeseen event. We have written Business Continuity Management Strategies (BCMS) in place which address issues that could arise in the event of any such emergencies. Areas we have covered include:

- Our premises becoming unavailable (fire, flood and other events of nature)
- Failure of key utilities (power, telephone network, internet access)
- Internal Server failure
- Staff contingencies (loss of key staff, pandemics and other events of nature)
- Emergency contact cascade

Should an unforeseen event arise we generally aim to restore full service within 2 working days. We will inform all customers of the disruption as soon as we are aware, ensuring that regular updates are provided to them in order to keep them informed. This would be done by website message and email.

Our BCMS policies are reviewed by Senior Management staff and tested annually to ensure they remain relevant.

As these documents contain business sensitive information, they are not available for external viewing.