CURTIS BANKS

GENERAL DATA PROTECTION REGULATION

UK - GDPR STATEMENT

JULY 2023

Accessing our services

If you experience difficulties accessing any of our services due to personal circumstances, we may be able to make some adjustments to help you. Please contact our SIPP Support Team on 01473 296969 or sippsupportteam@curtisbanks.co.uk to discuss any support adjustments that may be available to you.

Background

The Curtis Banks Group (the "Group"), administer SIPP, SSAS, and similar self-invested products, along with administration, and innovative technology solutions in the United Kingdom.

Commitment

The Group takes its personal information protection and data security responsibilities seriously; we are committed to protecting and enhancing the rights given to all data subjects for which we obtain, process and protect data in accordance with United Kingdom General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018 (DPA).

Summary

Under UK-GDPR/DPA, the Group continues to be both a Data Controller and Data Processor of Personal and/or Sensitive Data (this includes both personally identifiable information and special category information), which may be collected in certain specific circumstances.

We continue to review all feedback and Individual Rights requests received, alongside any relevant documentation we have in place.

This documentation sets out our obligations, the Individual Rights and the data stored, in respect of our Data Subjects.

Assessment

The Group collects, processes and uses only the minimum Personal and/or Sensitive Data in order to perform contractual obligations, and in accordance with regulatory and compliance requirements for the business activities we undertake.

Personal and/or Sensitive Data may also be shared within the Group to fulfil our internal and external contractual, and regulatory obligations.

In accordance with UK-GDPR/DPA, the Data Protection Officer (DPO) has overall responsibility to ensure our adherence of UK-GDPR/DPA within the Group, alongside the Risk & Compliance function.

CONTINUED

Responsibility

In line with the requirements of UK-GDPR/DPA, the Groups ongoing responsibility requires us to collect, hold and process Personal and/or Sensitive Data responsibly, by:

- Processing your Personal and/or Sensitive Data in accordance with the legal basis for which the data was originally collected.
- Ensuring that the Personal and/or Sensitive Data held, is accurate, and that there are processes in place to rectify any inaccuracies promptly.
- Maintaining robust security systems and controls to protect your Personal and/or Sensitive Data against unauthorised access, processing, loss or accidental destruction.
- Maintaining robust governance, operational procedures and ongoing employee training to maintain compliance with all data protection legislation.

Activity

The Group took initial action to align procedures, and processes with the GDPR when first implemented, as a result, the Group continues to enhance, and progress, to ensure we remain current, and at the forefront of the UK-GDPR, and the Data Protection Act (2018).

Initial Actions

- Information Audit: The Group carried out an audit of information previously held, to ensure that it was compliant with new UK-GDPR regulations.
- Policies & Procedures: The Group revised Data Protection Policies and Procedures to meet the requirements and standards of the UK-GDPR, and any relevant data protection laws, including:
    - **Data Protection**: The Groups Data Protection Policy and Procedure for Data Protection were revised to meet the standards and requirements of the UK-GDPR. Accountability and governance measures are in place to ensure that we understand, and adequately disseminate, and evidence our obligations and responsibilities, with a dedicated focus on privacy, and the rights of individuals.
    - **Data Retention & Erasure**: The Group updated all Internal and External Data Retention Policies to ensure that we met the 'Data Minimisation and Storage Limitation' principles, and that personal information was stored, archived and destroyed in accordance with our obligations (i.e. the Group has procedures in place to meet the new 'Right to Erasure' obligation).
    - **Data Breaches**: The Group ensured Data Breach Procedures had safeguards in place to identify, assess, investigate, and report Personal and/or Sensitive Data Breaches as quickly as possible.
    - **Third-Party Disclosures & International Data Transfers**: The Group ensured that you understood, that any Personal and/or Sensitive Data collected from you, or stored, could be transferred to a destination outside the UK, and that It could also be processed by our Service Providers (and their employees), operating outside the UK. We also took steps to ensure that in the event that your information was transferred outside of the UK by our Service Providers, appropriate measures and controls were in place to protect that information in accordance with applicable UK-GDPR, and Data Protection Laws.
    - **Subject Access Request (SAR)**: The Group revised its SAR Procedures to accommodate the revised 30-day timeframe for providing requested information, and for making provision, currently, free of charge.

CONTINUED

- **Privacy Information Notices (PIN's)**: The Group revised all Privacy Information Notices (PIN's), to comply with the UK-GDPR, ensuring that individuals who have had, Personal and/or Sensitive Information processed, had been informed of why we need it, how it is used, what their rights are, who the information is disclosed to, and what safeguarding measures are in place to protect their information.
- **Obtaining Consent**: The Group revised their consent mechanisms for obtaining Personal and/or Sensitive Data, ensuring that individuals understand what they are providing, why and how we use it, and giving clear, defined ways to consent to us processing their information.
- **Direct Marketing**: The Group revised the wording and processes for Direct Marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out, and providing unsubscribe features on all subsequent marketing materials.
- **Data Protection Impact Assessments (DPIA)**: Where the Group processes Personal and/or Sensitive Information that is considered high risk, the Group has developed stringent procedures for carrying out DPIA's that fully comply with the UK-GDPR Article 35 requirements. The Group has implemented documentation processes that record each assessment, allowing us to rate the risk posed by the processing activity, and implement mitigating measures to reduce the risk posed to the Data Subjects.

Summary

- The Group, and all its associated Procedures, Policies, Processes, Systems, and Controls, are fully compliant with the UK-GDPR.
- The Group has reviewed all of its own and third party contracts, and will (where applicable), further amend client and other third party contracts to ensure compliance with UK-GDPR, and the business activities of the Group.
- The Group will undertake Data Protection Impact Assessment (DPIA), and provide updated Privacy Information Notices (PIN's) where there are any significant changes to any of our products, services, processes, or changes to regulation, and/or legislation.
- The Group has updated all of its Privacy Information Notices (PIN's), in line with UK-GDPR requirements.
- The Group implements UK-GDPR specific content within internal Computer Based Training Modules, to ensure Group employees fully understand the requirements, and practices required under UK-GDPR.
- The Group will actively review its operational framework to ensure the Groups UK-GDPR approach is robust, and fit for purpose.