THOMSON REUTERS
KYC as a Service
END CLIENT COMPLIANCE WHITE PAPER

Due to the strictly confidential nature of the information managed through Thomson Reuters KYC as a Service we have implemented information security controls and management systems across a number of key areas to keep this information secure and in accordance with privacy and regulatory requirements.

This document explains our approach to information security and data privacy for KYC as a Service. It is designed to answer questions our end clients regularly ask.

DATA CENTERS

- KYC as a Service uses Thomson Reuters managed data centers in the United Kingdom.
- These are data centers are subject to an ongoing certification programme against ISO/IEC 27001.
- These are data centers are subject to an ongoing SOC 2 audit programme.

EXTERNAL AUDIT, ASSESSMENT AND CERTIFICATION

KYC as a Service has an ongoing Audit and Assessment programme:

- KYC as a Service has received independent assurance from Pricewaterhouse Coopers (PwC) against the ISAE[1] 3000 assurance standard, Type II. This provides an independent assessment regarding the design effectiveness of our internal processes and controls over a period of time of live operations. Regular Type II reporting will take place through the lifetime of the service.
- Regular penetration testing by an independent third party company.
- Regular scanning of code and infrastructure using third party capabilities.

STAFF

All KYC as a Service Operations staff are subject to pre-employment background screening, security awareness training, and the Code of Business Conduct and Ethics.

Employment contracts include specific clauses governing employees' obligations of confidentiality and obligation to comply with the Thomson Reuters Employee Code of Conduct.

Staff are trained on specific KYC as a Service workflows and procedures and their work is subject to specific KYC as a Service information security policies and procedures.

[1] International Standard on Assurance Engagements

POLICIES AND STANDARDS

Our information security policy is endorsed by the Thomson Reuters Executive Committee and outlines the security principles that apply to our People, Processes and Technology that address all aspects of our service delivery. These policies and standards are regularly reviewed to take account of evolving technical risks as well as regulatory changes and our customers' needs for information security. They cover:

- Product Assurance
- Infrastructure Security
- Virus Protection
- Patch Management
- Incident Response
- Device Lockdown
- System Monitoring
- Vulnerability Scanning
- Risk Management and Business Assurance
- Privacy and Regulatory Compliance
- Physical Security
- Business Continuity & Disaster Recovery

NETWORK SECURITY

The Secure protocol (TLS) is used to encrypt network communication for all sensitive traffic. Strong authentication is used to control access to sensitive information and services relating to strictly confidential information. KYC Operations team connectivity to the production systems is over internal Thomson Reuters network. No VPN access is allowed here.

INFRASTRUCTURE SECURITY

The KYC as a Service technology is deployed in a dedicated zone in a segregated network infrastructure with appropriate access controls.

APPLICATION SECURITY

The KYC as a Service application implements the following information security features:

- Authentication with secure session management
- Password standard
- Entitlements based on strict security groups, role assignment and user-level keys
- End Client permission is required before a financial institution can view their KYC as a Service record
- Anti-virus scan of all documents coming into the service
- Data and document encryption designed into the application architecture (data encryption at rest and document encryption through the application)
- Audit logging of all actions on information managed through the service

RECORD PROCESSING CENTRE SECURITY

Physical & environmental security

A number of measures have been adopted to ensure the risk of tampering with equipment is minimized. Information is only visible to authorized dedicated personnel. There will be appropriate supervision of staff working with sensitive data.

Device security and malware protection

KYC Analysts have a terminal dedicated to their analyst work. This is extensively locked down allowing only essential access to network resources and the internet. Access to removable media, wireless and printers is disabled and the analysts have no local administer rights.

KYC as a Service record processing center policies

- No remote working on sensitive information is possible or permitted
- No corporate or personal mobile devices permitted within the record processing area
- No hardcopies, printing, local saving or other extraction of sensitive information is permitted

BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

Business Continuity refers to the people, processes and locations in place to provide continuity of service in the event of a disaster. Disaster Recovery refers to the technical recovery of the applications that both customers and KYC as a Service staff utilize as part of KYC as a Service.

Business Continuity (BC)

- The Business Continuity (BC) Plan for KYC as a Service is based on one of the record processing centers being unavailable to KYC as a Service staff (for example due to fire, power or communications failures).
- The KYC as a Service BC plan is tested frequently, at a minimum of annually.
- The Business Continuity Plan and its testing are in scope of the external ISAE3000 Audit.

Disaster Recovery (DR)

- KYC as a Service applications and data reside in two Thomson Reuters managed data centers in the UK, one in London and one in Hampshire.
- Data are securely synchronized between the centers.
- Onsite backups are performed in each data center.
- The RTO (Recovery Time Objective) for the application is 4 hours, and the RPO (Recovery Point Objective) is 30 minutes.
- DR is tested at a minimum of annually.

PRIVACY AND REGULATORY COMPLIANCE

KYC as a Service is a Data Controller in the UK for the Managed Service and a Data Processor in the UK for the Document Exchange.

Governance

- Privacy Controls in KYC as a Service comply with Thomson Reuters Global Data Privacy Guidelines. Our internal controls reflect the requirements of applicable local data privacy laws including those which require express consent for the processing of personal information.
- Thomson Reuters has a dedicated Corporate Privacy Team who manage our global standards and procedures as well as data privacy officers in our key international markets. Clients of KYC as a Service also have the support of a dedicated KYC as a Service Privacy Officer who helps to ensure that personal data collection, use and sharing is transparent and open in order to meet the requirements of applicable data privacy law.

Consent

Consent for obtaining and processing non-publically available personal data within KYC as a Service is obtained via a written consent procedure which is a requirement of uploading personal data into the system. The means that all individuals whose non-public personal information is uploaded understand how it will be used, transferred and otherwise processed. In addition it ensures that they have provided their explicit consent to allow their personal data to be shared with Clients of KYC as a Service.

Data Quality

Controls are in place to ensure data quality. Controls are also in place to ensure that retention periods based on local laws are applied and personal information is retained in the KYC as a Service database only as long as necessary to comply with reasonable business needs of applicable legal retention periods.

Data Subject Rights

Individuals and Swiss Companies have full rights of access to their information held in KYC as a Service. Access requests to the information held in KYC as a Service will be subject to UK data privacy laws and requests for information will receive a response within 40 days.

Data Transfers

We understand that due to the international nature of many of our Client's businesses the personal information in KYC as a Service may be transferred across geographical boundaries. Individuals are informed of this when they upload their data into our system and any data transfers are based on the individual's consent. Further, we also sign additional data transfer agreements with our Clients based on European Model Clauses, CBPRs or other legal requirements when local laws require this. Internal data privacy agreements are also in place to protect our internal data flows.