THOMSON REUTERS LEGAL TRACKER

FORMERLY SERENGETI TRACKER

legal-solutions.co.uk/legaltracker

Data security and certification what you need to know about Legal Tracker's UK data centre

QUICK FACTS

- Data Centre is ISO27001 certified
- 2014 SOC 2 and SOC 3 audit reports
- Annual third-party penetration test
- Data is encrypted in transit and at rest
- Disaster recovery

the answer company™
THOMSON REUTERS®

Data security and certification what you need to know about Thomson Reuters Legal Tracker's UK data centre

Thomson Reuters has invested in establishing a UK data centre to support further expansion of the Legal Tracker business in Europe. This investment will enable clients to store their data securely in the UK. It is this level of investment that helps ensure Legal Tracker is the most highly rated e-billing, matter management and reporting solution for in-house counsel today.

Legal Tracker has a demonstrated history of implementing data security best practices combined with independent third-party assessments to validate that the security controls are both appropriate and operating effectively. The security and availability of your data is our priority.

ISO 27001 CERTIFICATION

What is ISO 27001?

ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

ISO 27001 was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.

ISO 27001 uses a topdown, risk-based approach and is technology-neutral. The specification defines a six-part planning process:

1. Define a security policy
2. Define the scope of the ISMS
3. Conduct a risk assessment
4. Manage identified risks
5. Select control objectives and controls to be implemented
6. Prepare a statement of applicability

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organisation.

SOC 2 AND SOC 3 AUDIT REPORTS

SOC 2 and SOC 3 audit reports have been carried out to include physical and environmental controls.

What is SOC 2 compliance?

SOC 2, pronounced "sock two" and more formally known as Service Organisation Control 2, reports on various organisational controls related to security, availability, processing integrity, confidentiality or privacy. The standard for regulating these five issues was formed under the American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria and it is recognised worldwide as one of the strictest audit standards for service providers.

This certification has been designed to meet the needs of the growing number of IT and cloud computing companies. It allows Legal Tracker to demonstrate that it meets and exceeds the industry's accepted standards governing controls and protection of all hosted and processed data, on behalf of clients.

UK DATA CENTRE SECURITY

Legal Tracker's primary data centre is based in London with the secondary, disaster recovery site in Fareham. Each site includes environmental features like backup generators, state-of-the-art fire suppression and water-detection systems, 24/7 security guards on staff and video surveillance and biometric access controls, to name a few.

Data security and certification what you need to know about Thomson Reuters Legal Tracker's UK data centre

SERVER SECURITY

Servers are hardened prior to deployment through the use of best practices (i.e., disabling unnecessary services) and applying approved patches. All servers are monitored programmatically for changes, and all changes are reconciled against the record of approved change requests. All changes to systems adhere to Thomson Reuters Change Management policy to ensure that changes are tested, reviewed, and approved prior to application to production systems.

Servers are segmented into roles, with each role having a specific network that it resides on and limited or no access beyond its assigned network.

APPLICATION SECURITY

To ensure against co-mingling of client data, Legal Tracker provisions each client with a dedicated database. Data stored in the databases is encrypted at-rest to further protect customer data against loss. The Legal Tracker application is built upon the principle of permissions. User accounts are created and administered by the customer. New accounts receive an email with a one-time-use link that will require the user to set a password upon using the link. User accounts are provisioned access to matters by a customer account with appropriate permissions. Users can only see the data to which they have been granted access. Legal Tracker enables customers to configure password requirements to mirror their own corporate password policies.

From a supported Web browser, customers connect to Legal Tracker via an HTTPS session that is secured with 128-bit encryption certification, thereby enforcing encryption of data in transit. At the customer's request, Legal Tracker can enable IP restrictions that limit the ability of customer users to log in to Tracker only from their corporate network or through their corporate VPN.

MONITORING

Multiple monitoring strategies have been implemented to allow Legal Tracker to monitor the entire infrastructure from a variety of different angles to enable a full view into the performance of the environment. Automated monitoring is configured to programmatically page the on-call personnel in the event certain thresholds are reached and to enable prompt resolution.

DISASTER RECOVERY

Legal Tracker uses a multi-phased approach to enable the recovery of customer data in the event of a disaster. Disk-to-disk backups are utilised to eliminate the need for storing tapes off-site. Both data and backups are replicated to the disaster recovery site to offer the maximum flexibility for recovery in the event of a disaster. Failover testing at the disaster recovery site is performed at least twice a year.

Thomson Reuters provide legal solutions for corporate counsel and the legal profession as a whole. To hear more about Thomson Reuters Legal Tracker or to arrange a demonstration on the service, please contact:

EMAIL: **legaltracker.info@thomsonreuters.com**

VISIT: **legal-solutions.co.uk/legaltracker**

3431601A/April 2016