Thomson Reuters and the GDPR

Thomson Reuters has a long history of providing reliable and trustworthy information to our customers. Integral to how we do this is our commitment to privacy and how we protect personal data. This document answers questions our customers often ask about how Thomson Reuters is preparing for the GDPR.

Our commitment to privacy

As a company that prides ourselves on customer trust, the protection of personal data and compliance with applicable privacy laws (including the GDPR) are key priorities at Thomson Reuters and fundamental considerations in how we operate as a company. We have implemented a number of technical, organisational and legal mechanisms to protect personal data, which have been proactively reviewed and updated in light of the GDPR.

This commitment is driven by our global team of privacy experts that oversee the use of personal data in our products and services, working in close collaboration with our information security and technology teams.

In addition, this commitment is recognized by all Thomson Reuters employees and contractors through our Code of Business Conduct and Ethics, which details the obligations we place on our staff with respect to confidentiality, information security, and privacy compliance. We have built our Code of Conduct on our purpose and our values so that the way we collect, use, retain or transfer personal data is aligned across our business and meets best practice

What we are doing to prepare for the GDPR

We fully recognize the importance of the GDPR to our business and, most importantly, to our customers. In 2017 we launched our privacy compliance program, Privacy Matters, to ensure our readiness for the GDPR. As part of Privacy Matters, we have invested significant time and resources into evaluating our products and services, as well as refreshing functionality, support processes, product descriptions, marketing material, data governance and security policies and data protection practices. This investment is designed to ensure that we are ready for the GDPR and offer our customers products and services that help them meet the challenges presented by the GDPR.

Privacy Matters is looking at the GDPR across the full spectrum of our business and includes a review of all aspects of our privacy and information security compliance including: identification of data processes, risk assessments, as well as updates to data governance structures, policies, notices, records, procedures, training and customer and vendor agreements.

The program is sponsored by our Chief Technology Officer, General Counsel, and our Privacy Office and involves input from stakeholders across our business, including product owners, technologists, information security, our legal department, and many others. This multi-stakeholder approach allows our Privacy Matters program to embed enterprise-level processes and a company culture designed to promote GDPR compliance not only for May 2018, but beyond.

Data governance and security framework

Privacy compliance across our organization is led by our Privacy Office and Chief Privacy Officer (CPO). Our CPO is located in the United Kingdom and reports directly to the General Counsel of Thomson Reuters. She also plays a leading role in our Privacy Matters program. The Privacy Office (with members in the United States, Europe, and Asia) supports our organization with continual up-keep and development of our policies, processes, practical guidelines and training on processing and protecting personal data. Our Privacy Office is also on hand to advise our business on privacy and information governance on a day-to-day basis. Our privacy compliance program is further supported by a team of nearly 200 Thomson Reuters legal professionals across the company and around the world.

Our Chief Information Security Officer (CISO) leads our Information Security Risk Management (ISRM) program. Our extensive, global ISRM team is responsible for our security controls, security framework, and audit of those controls. Our CISO and ISRM team ensure that products, applications, platforms and infrastructure are protected, and customer data are safeguarded. ISRM has been integrally involved in the Privacy Matters program and their expertise has been critical in ensuring that our commitment to the GDPR focuses on the technical security controls and measures required to appropriately protect personal data.

THOMSON REUTERS®

The involvement of our senior management in the Privacy Matters program has made certain that privacy and information security also have the full attention of the Thomson Reuters Board of Directors and further demonstrates the scale of this commitment across the company.

Our approach to customer contracts

Many of our products handle personal data and we recognize that our customer contracts need to be updated to meet the requirements of the GDPR.

As part of the Privacy Matters program we are proactively updating existing contracts to provide additional privacy protections in line with the GDPR. This includes making contractual commitments to our customers to satisfy the requirement of Article 28 of the GDPR where Thomson Reuters acts as a processor of customer personal data. These new terms and protections are purely additive and do not alter or impair any rights that our customers may have in their current contracts with us. These additional terms include our commitment to keeping customer personal data secure and confidential, and help our customers to understand our use of sub-processors, what customer personal data we hold, how we process this personal data, and how we will assist our customers in complying with their own GDPR obligations.

We are also introducing revised and expanded data protection provisions into our new customer contracts. These provisions are designed to ensure that our customers have a contract with us that satisfies the requirements of Article 28 GDPR where relevant and includes appropriate additional privacy protections.

The exact nature of our commitments to a customer will vary depending on whether Thomson Reuters is a data controller or a data processor of the personal data that it holds. Our respective roles and responsibilities, along with further information about our products, are set out in our GDPR product information, which is available at www.tr.com/privacy-information. For some of our products, more detailed privacy and security information may also be available on the site.

Our contractual approach reflects the products and services we provide as well as our technical environments and operational procedures and policies. A consistent approach allows us to fulfil our obligations under GDPR, whilst continuing to ensure we provide high quality services to all or our customers. The stability, integrity, and compliance profile of our products and services also rely on this harmonized approach towards our information security and data protection methodologies.

Our commitment to information security

Thomson Reuters understands the importance of keeping personal data secure and our information security policies and practices are a fundamental part of this commitment. We use data classifications to ensure that security protections are appropriate to the level of risk attaching to data we are protecting. Additionally, our security strategy includes appropriate security controls are communicated to application owners and technology teams across the business to support the secure development of products and a secure operating environment. This is all done to mitigate threats to the confidentiality, integrity and availability of customer data which we store, process or transmit.

Our ISRM function supports a program that includes:

Security Monitoring

Security logging and monitoring of the operating environment for the purpose of awareness, event correlation, and incident response.

System Monitoring

Monitoring of critical systems, services and operations are implemented to ensure the health of the operating environment on which our products run.

Vulnerability Scanning

Our ISRM team supports a vulnerability scanning and policy compliance service which can be utilized by product and technology teams for internal or external vulnerability scanning and configuration compliance. Internet-facing sites on our global network are periodically scanned as part of our vulnerability management program.

Encryption

Our internal Information Security Policy requires that sensitive data, including customer, partner, and regulated data is encrypted when it is in transit over public networks and in certain circumstances when it is stored (at rest).

Patch Management

We gather and review security threat intelligence from our vendors and other third party security organizations. The patch management standard provides appropriate patching practices to technology teams for deploying security

patches. At times, additional security controls may be implemented to provide mitigation against known threats.

Virus Protection

All Thomson Reuters-owned and supported operating systems that are hosted in our data centers or managed at customer sites are required to be configured with Thomson Reuters' antivirus solution for compliance with our policies and standards. This excludes operating systems that are not managed by Thomson Reuters.

Infrastructure Security

Our products and services are offered through public and private networks. There are tiered controls, including the use of network segmentation, to ensure the appropriate level of protection to systems and data.

Device Lockdown

Standard server builds are deployed across our infrastructure. Our builds are based on industry practices for secure configuration management.

Physical Security

All strategic data centers are managed to the standards within Thomson Reuters Corporate Security Policy guidelines based on best practices in the industry. These guidelines include requirements for physical security, building maintenance, fire suppression, air conditioning, UPS with generator back-up, and access to diverse power and communications. Thomson Reuters policy requires that each and every facility be subject to comprehensive audits.

A variety of secure methods are used to control access to Thomson Reuters facilities. Depending on the sensitivity of the facility, these methods may include: the use of security staff, ID cards, electronic access control incorporating proximity card readers, pin numbers or biometric devices.

Our information security program (including our infrastructure, technical controls, processes, policies and certifications) is also reviewed and updated periodically considering technical risks; regulatory changes and our customers' needs for information security.

Access controls

Thomson Reuters policies require identity and access controls to enterprise resources, product environments and applications which adhere to established industry standards including least privilege, segregation of duties, unique IDs, password management, and privileged access management. This helps to ensure that access to information by our personnel and the personnel of our customers is appropriately limited.

Access to our production networks and production systems is also governed by technical controls that require multi-factor authentication and unique IDs.

Our information security risk assessment methodology

Our product and technology teams engage information security subject matter experts regularly to provide risk assessments services. Architecture reviews, vulnerability scans, application security testing and technical compliance reviews are several of the services performed during risk assessment activities.

Following risk assessment activities our ISRM team consults with product and technology teams to develop remediation plans and roadmaps to address any gaps or areas of identified risk. Additionally, our internal compliance team performs audits against policies, standards and regulatory requirements, and registers findings for review and remediation initiatives. These processes are designed to maintain and improve the information security and privacy compliance profile for Thomson Reuters and our customers.

Audit and accreditation

Our information security policies and standards are aligned to an international standard on information security best practice. This provides our customers with comfort that we have in place robust practices that ensure the confidentiality, integrity and availability of our products and services. Our products undertake comprehensive application security testing, which includes performing static and dynamic application security testing and third-party penetration testing.

To further demonstrate our commitment to delivering a secure operating environment for our business and our customers, we maintain ISO 27001 certification for our strategic data centers. We provide customers with relevant information to support them in confirming the appropriateness of our information security and privacy measures. This can include third party audit reports, details of certifications and other documentary information. For example, we may engage with independent third party auditors to carry out SOC2 audits and provide customers with information on the audit.

To safeguard the integrity, security and confidentiality of our systems and the information provided by our customers, our policies do not permit customers to carry out an audit.

Supply chain verification and vendor contracting

Thomson Reuters is a global company offering a vast array of products around the world. In order to operate our wide-ranging business and deliver our products to a global customer base, it is important that we are able to freely use subcontractors. We have a strong onboarding process in place to verify the suitability and integrity of these subcontractors and employ contractual agreements to ensure that data transfers and data processing is undertaken in a secure and authorized manner. In addition, we require that all subcontractors adhere to the Thomson Reuters Code of Business Conduct and Ethics which requires all contractors, temporary workers, vendors and outside agents to comply with our privacy and information security policies and practices. As part of the Privacy Matters program, we are updating our vendor contracts to ensure that they meet the standards set by the GDPR.

Our employees and contractors

Our Code of Business Conduct and Ethics includes detailed sections on privacy and information security, and all employees and contractors are bound to adhere to these. Employees and contractors who fail to abide by these privacy and information security policies are subject to disciplinary action, up to and including dismissal. Privacy and information security training is mandatory for all employees and contractors who handle personal data.

Thomson Reuters takes steps to ensure that only appropriate persons access personal data. Relevant Thomson Reuters employees and contractors must complete pre-employment background screening checks and comply with confidentiality provisions placed upon them. Each employee is provided access only to the appropriate premises and systems once they complete these checks. Controls are also in place to monitor, review and adjust access as appropriate. Should an employee or contractor leave Thomson Reuters, access to systems and premises are terminated.

Location of personal data and overseas data transfers

Thomson Reuters is a global organization that provides 24/7 solutions. In order to accomplish this, we use a global team to provide services, support and maintenance. This means that personal data may be stored in or transferred to countries outside of the European Economic Area (EEA). Any such transfers are performed only in compliance with the applicable data protection laws (including the GDPR).

To adequately protect personal data transferred between different entities within the Thomson Reuters entities in and outside of the EEA, each member of the Thomson Reuters Group signs up to and complies with an Intra-Group Agreement (IGA) with EU Model Clauses provisions. Our IGA helps to ensure a consistent framework and standard for the transfer of personal data throughout our entire organization. In addition, we enter into appropriate contractual agreements with our vendors to ensure that data transfers are undertaken in a secure and authorized manner.

Data breaches and security incident response

Thomson Reuters implements appropriate measures designed to prevent personal data breaches based on applicable legal requirements, such as the GDPR, which are continually reviewed and updated as necessary in view of regulatory changes. These measures include architecture reviews, vulnerability scans, application security testing and technical compliance reviews.

An incident response process exists to address incidents as they are identified. If an incident should occur, we have a process in place to take swift action and mitigate impacts. These actions may depend on our role in relation to the product or service, for example, whether we are controller or processor of the personal data. Incidents are managed by a dedicated incident response team which follows a documented procedure for mitigation and communications. In each case, we work together with affected parties to minimize effects and to take action to prevent future breaches. We have outlined responsibilities in case of breaches in our contracts, both with customers as well as with vendors.

Data subject rights and requests

Under the GDPR, individuals (data subjects) have various rights relating to how their personal data is managed. They may, for example, have the right to access, correct or restrict the use of personal data, or they may object to processing or request deletion of certain personal data. Thomson Reuters has a comprehensive process in place to deal with these data subject requests. Our actions and responsibilities will depend on whether we are the controller or processer of the personal data at issue.

Depending on the product and our role as either a controller or processor, the process for enabling these data subject rights may differ, and are always subject to applicable law. For many products, we offer a self-service option that allows customers to access, correct, or delete the personal data that they or their users may have entered, allowing the customer to respond to data subject requests directly. For any products where self-service functionality is not available, we have functionality in place that will allow us to assist customers in complying with their obligations to respond to data subject requests. Please contact our Privacy Office at privacy.enquiries@tr.com if you have a specific need for assistance with a data subject request.

Business continuity and disaster recovery strategy

Thomson Reuters is exposed to an increasing array of potential risks that could impact critical business functions or services following a disruptive incident. The goal of our Business Continuity and Disaster Recovery strategy and plans is to ensure our continued ability to serve our clients and to protect our people and assets.

We have an established global, structured framework, designed to ensure that Thomson Reuters is prepared should a disruptive incident occur. This approach addresses disruptions of varying scope, including, but not limited to, large-scale location-specific events and Thomson Reuters-only disruptive incidents.

Central to our efforts is a requirement that each Thomson Reuters business unit develops, tests and maintains business continuity plans for each of its critical functions. Our strategy and plans include leveraging our global resources and infrastructure based on business requirements and as dictated by the specific crisis event.

We prioritize systems recovery based on the criticality of the systems to our clients; then, recovery requirements are established based on those priorities. As a further safeguard, many critical functions can be transferred to out-of-region locations. Additionally, Thomson Reuters can support many critical functions by enabling designated staff to work from their homes through secure remote-access connections. Integral to our business continuity readiness is employee awareness and training so that employees are aware of their roles and responsibilities in the event of a disruptive incident. In accordance with business requirements, and as part of our regular maintenance, stringent testing of systems failover/recovery and business continuity sites and plans is conducted on a recurring basis, which increases the confidence of our business continuity readiness. Associated strategies and plans are required to be reviewed and updated at a minimum on an annual basis.

Back-up, data retention, and secure disposal

We have internal policies that govern the back-up of client data at appropriate intervals depending on how that data is classified. Back-ups are done securely and stored in our secure data center locations or with carefully-selected hosting providers who have undergone our stringent security screening and vendor onboarding process.

Our dedicated records management team maintains our records retention policies, which includes requirements to periodically delete customer data from our systems in compliance with the GDPR or other applicable law. The records management team works with our ISRM team and our Privacy Office to align policies and controls with legal and security requirements.

Our data retention and destruction obligations depend on our role when providing a specific product or service. To the extent that Thomson Reuters is a data controller, we have adopted procedures and technical safeguards so that personal data is retained in accordance with applicable laws, including the GDPR. To the extent that Thomson Reuters is a data processor, customers are responsible for setting, and respecting, appropriate retention periods for the personal data that their users have submitted. Many of our products include controls and functionality that can help customers comply with their obligations around the retention and deletion of personal data.

Following the expiry or termination of a customer's contract for a product or service, Thomson Reuters securely

returns, anonymizes, or deletes customer data (including personal data) in line with its contractual obligations and will only continue to retain such data where required to do so by law.

For more information

If you would like to know more about our approach to processing and protecting personal data in line with the GDPR for specific products, please visit www.tr.com/privacy-information.

For general questions on how Thomson Reuters deals with privacy, or if you have suggestions or concerns, please contact us at privacy.enquiries@tr.com.

General information about Thomson Reuters can also be found at http://ir.thomsonreuters.com.