Thomson Reuters and the GDPR

The program is spo
General Counsel, a
from stakeholders a
owners, technologis
department, and ma
approach allows ou
enterprise-level pro
designed to promot
2018, but beyond.

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.

we are doing to prepare for the GDPR

GDPRPRPD 13 > Hallgarten GDPR

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

Data governance and security framework

and offer our customers products and servi

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

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 (s)e413 0 Td -2.6(3.4(pdat)15(s)4(ifd5)5T.d(ar)3.7wr)33.4 tmfu.4(ed .3(i)-0.7(c)2.6(e)13ni)12.6(es)

THOMSON REUTERS