Cloud Services

SDL Limited (“SDL”)(for and on behalf of its affiliates and subsidiaries) a part of the RWS Holdings Plc group.

Privacy Policy for software licensed under the RWS Suite of SaaS Products.

Author: VP Cloud Operations

Approver: Head of Group Legal Services

Version: 1.0

Issue Date: 01/03/2022

Next Review Date: 16/01/2023

Classification: Public

Retention Period: Six years after updated

Contents

1 Document history

Author or Reviewer (to be completed by the author or reviewer)

Name	Date	Detail (identify changes made and pages affected)
Data Privacy Officer		Creation from SDL original version 1.12

2 Scope

This SDL Privacy Policy is an appendix to the Master Subscription Services Agreement to give customers insight into security measures SDL has in place to assure confidentiality, integrity and availability of Customer's information.

This Policy shall be deemed to take effect from the Effective Date of the Master Subscription Services Agreement and shall continue in full force and effect until the termination of the Agreement or return of all information assets to the Customer or deletion of the data has occurred.

This Policy applies to the services available in SDL Cloud. The Policy describes the level of privacy and data protection SDL undertakes to maintain for the security of data during data processing. This policy covers all SDL Core Products available via SDL Cloud. In terms of the GDPR and UK DPA, SDL operates as a Data Processor of data, for which the Customer is the Data Controller.

In addition to this Policy, a Data Processing Agreement as necessary can be added as an Addendum, for our customers for which SDL processes information.

The Policy is based on industry best practices, and fulfills an important role in executing the European General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (UK DPA)

Details on how SDL employees handle personal Customer information are set out in security policies and procedures. These documents are classified as SDL Internal and therefore only available for RWS representatives.

In addition to this Privacy Policy for Cloud Services information about collecting, processing or handling personal information can be found on RWS's corporate website: https://www.rws.com/legal/privacy/privacy-notice/

3 Terms & Definitions

Terms in the Master Subscription Services Agreement shall have the same meaning when used in this privacy policy. In addition, definitions below apply in the document.

Customer	The customer who purchases Services from SDL, listed on the executed Master Subscription Service Agreement
DPL (Data Protection Law)	Means the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and the UK Data Protection Act 2018.

Data subject	Means any identified or identifiable natural person as defined in the DPL.
Data controller	Organization that determines the purpose and means of the processing of Personal Data, having the ability to decide how Personal Data is collected, used, altered and disclosed.
Data processor	Individual or organization that processes Personal Data on behalf of the Data Controller.
Personal Data	Means personal data as defined in the DPL that the Data Processor (SDL) processes on behalf of Data Controller (Customer) in connection with the Master Subscription Services Agreement
RWS	Means RWS Holdings Plc and its subsidiaries and affilaites.
SaaS Products	Specific SDL Products provided in a Cloud environment, with related information storage capability for the use of the Licensee, provided solely for storage of data used in the product or generated through use of the product.
Services	The Service SDL will provide is the provisioning, management and service delivery of specific Enterprise SDL Products.

4 Policy

4.1. Scope and Categories

This policy describes the processing of personal data in Services and SaaS products offered by SDL as Data Processor. In general, SDL provides the products as is and the customer has to determine the type of data which they will process. General terms for data handling can be found in the Acceptable Usage Policy in the Master Subscription Services Agreement Schedule B.

However, it is recognized that in some cases Customers do require the ability to process personal data. When required, such processing will be contractually agreed. The details on processing of personal data are provided below for information as applicable. If a Customer chooses to process data of a type not contractually agreed RWS must be notified in advance and potential new solutions and/or data handling mechanisms need to be established as appropriate.

The Software applications are offered as a service and will potentially collect (collection occurs in respect of authentication and usage but also in respect of Customer data in limited and strictly defined conditions restricted to named applications), process and use personal data.

The Data Controller determines the purpose for which the data is processed, initiates and controls the processing. SDL provides or configures the Software to enable the Software to perform such processing

in accordance with the Customer's instructions. SDL shall not use the personal data for any other purpose than those agreed with the Customer.

In Schedule 1 we list the SDL Software products and whether the Software processes/stores personal data. (Note: in all instances the security applied will be the standard of security SDL describes in this Policy)

In respect of all Software:

i. **All services, applications and components will collect Personal Data based on service usage. This (technical) log-information is collected only for systems administration, troubleshooting and fraud monitoring purposes. Log-information will only be disclosed outside of the RWS Group of companies if SDL opt to use third-party tools for the purpose of log aggregation. These third-party tools maybe cloud hosted hence the data may be transferred to a third party running the service on RWS's behalf.**
ii. **Authentication data provided to RWS to enable access to the Software either for administrative purposes or processing may contain Personal Data which is only obtained for the purpose of authenticating access to the Software and license management.**

The nature of the data, which the Service can be used to transmit or disseminate, is restricted and varies by product. The details of the restriction appear in the Acceptable Usage Policy at Schedule B of the MSSA.

4.2. Locations and 3rd party service provider

RWS uses third party service providers for its infrastructure and platform services. All RWS service providers follow the highest industry standards (for example certified on ISO27001 or SSAE 16 SOC 2) on physical and information security. In Schedule 2 we list the subcontractors used for hosting services and their datacenter locations for data storage. Backups of databases containing Personal Data are stored in a secondary location for business continuity purposes.

Services generate log-information, which is stored and processed at the same datacenter as the service is running (but see comment on log aggregation above).

SDL employees undertake all application and system administration together with third party service providers of their element of the infrastructure. As part of Service delivery, SDL employees may process personal data on behalf of the Customer (Data Controller).

4.3. Data transfers

SDL has in place approrpriate safeguards and approrpriate frameworks to enable international transfers of data and RWS has entered into appropriate contractual arrangements with third party providers to ensure adequate protection of personal data.

Electronic offsite backups as described above are transferred between different SDL datacenters provided and stored by the same third party, such transfers take place over a private link between the data centers.

Data is not transferred or shared between different SDL customers.

If SDL receives a demand from a law enforcement agency to disclose Customer's Personal Data or Personal Data provided by the Customer, where possible, SDL will direct the law enforcement agency to

Customer, providing the Customer's basic contact information. SDL will inform Customer, unless prohibited, of a law enforcement agency's request to access personal data. If SDL is compelled to disclose data, SDL will comply with the obligation to disclose and unless prohibited inform Customer afterwards. RWS's legal department will consider any such requests received and determine SDL's response.

4.4. Data security

For security of personal data a layered architecture is implemented which facilitates different platform, infrastructure, and/or application layers. The following paragraphs give Customers an overview of security measures.

Physical Security

For platforms and infrastructure, SDL uses IaaS and PaaS services from, Amazon Web Services and Alibaba,. These companies comply with highest industry standards (ISO 27001 and/or SSAE 16 SOC2) for both information security and physical security.

Platforms and Infrastructure management

All data in transit over public networks is secured by use of encrypted protocols (e.g. HTTPS, SFTP, etc.). Communication between components in different locations (i.e. source and destination) traverses RWS firewalls.

All communication between end-users and services is secured with encrypted communication. Independent and trusted 3rd party digital certificates are used on services to prove integrity and identity of the service.

Infrastructure and platforms are periodically tested for vulnerabilities, by industry standard vulnerability assessment tests. Besides testing, SDL services are secured by anti-virus and anti-malware software (where required and security risks are identified). Updates to operating systems, anti-virus, anti-malware and applications are installed via a patch and release management process on a regular basis.

Multifactor authentication on management interfaces is active for system administration at Amazon Web Services.

Encryption of data at rest can be achieved by enabling the encryption at VM or storage level where supported.

System administrators follow policies and guidelines when administering systems containing Personal Data. These policies are part of the RWS Security Program and updated regularly. As part of ISO 27001 certification controls are implemented in certain parts of the organization (see below).

ITIL processes are implemented within the Cloud Operations and Service Delivery department for incident, change and release management.

Managed services department

As a part of managed services, SDL employee's access to Customer data including Personal Data is restricted. Only the Cloud Operations and Service Delivery teams can perform management of the Services during which they will have access to the Personal Data stored. These employees receive additional training on handling personal and/or Customer data. In any event processing of any Personal Data is only performed on behalf of the Customer as described in the Master Subscription Services Agreement. Administrator access is granted as needed, using the "Least Priviledge Principle". Administrator access rights are reviewed at regular intervals.

4.5. Data Deletion

Within 42 days of termination of the Agreement, SDL will securely delete Customer's data. Before secure deletion when agreed, SDL can provide a copy of Customer's data to Customer, (SDL reserves the right to charge a fee), after which Customer's data will be securely deleted in accordance with policies.

Backup – Data Rotation

AWS	EBS volumes are backed up every day & stored in S3 with retention period of 30 days. This backup goes into destination region which confirms that all data prior to the 30 day period will be deleted from the system. On AWS, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Alibaba	Alibaba cloud disk volumes are backed up every day with maximum retention period of 30 days.

Account Closure

When an account comes to an end of engagement with SDL; all data related to the customer can be transferred back to the customer upon request and all resident data/systems are securely removed from the system in accordance with the time frames described above.

4.6. Privacy and security awareness within RWS

Privacy Training

Within the Cloud Operations and Service Delivery teams, all employees receive both mandatory privacy and security awareness training throughout the year. Different topics are covered, with content mapped to the job role of the employee. This training is undertaken in addition to the annual general security awareness training. Attendance and effectiveness is monitored and tracked for audit purposes.

Information Security Team

The Chief Technology Officer is the executive sponsor for security at RWS and is responsible for the security strategy. RWS' security program is managed on a daily basis by the Head of Security Risk & Compliance and the information security team who continually monitor and report on the effectiveness of security controls; carry out independent information security audits; deliver security training and awareness; and provide specialist information security consultancy to development and operations teams as well as the remainder of the organisation.

Data Privacy Officer

RWS's Data Privacy Officer provides advice on the confidentiality and integrity of Personal Data within the SaaS products and implements and maintains the Privacy Policy. The Data Privacy Officer must hold, or be working towards, a Certified Information Privacy Professional – European Union (CIPP-E) and Certified Information Privacy Professional – United States (CIPP-US) certification and should attend training and conferences to keep knowledge up to date.

All these roles work closely to ensure the confidentiality, integrity and availability of Personal Data is maintained.

4.7. Rectification and Data Subject Requests

Rectification, deletion and blocking of data: The accuracy of the data is the Customer's responsibility. Any request from a Data Subject directly to SDL, will be directed to the Customer and SDL will provide the Data Subject with basic contact information for the Customer. As SDL is not involved in the processing of the detail of the data, SDL does not anticipate undertaking any rectification, deletion and blocking of data, which is the responsibility of the Customer.

However, if Customer does require SDL to undertake such rectification, deletion and blocking of data, SDL will undertake such work upon agreement with the Customer in a Statement of Work and SDL being paid for the work undertaken at the then prevailing SDL Professional Services rate.

Please note, that where the removal of such data means the contractually agreed upon activities between SDL and Customer cannot be performed, or puts other individual Personal Data at undue risk for exposure, SDL retains the right to deny the request. A formal description of reasoning can be supplied upon request.

4.8. Further Information Contact

If there is any question, comment, or concern about this Privacy Policy, please contact us as follows:

RWS Holdings PLC

Europa House
Chiltern Park
Chiltern Hill
Chalfont St Peter
SL9 9FG
England
FAO: Privacy Officer (Legal Department)

Email: privacy@rws.com

4.9. Data breaches

A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed in connection with the provision of a service provided by SDL.

SDL's service desk will inform Customer via e-mail as soon as possible after detection of an actual or suspected Personal Data breach. Additionally, SDL will notify appropriate Regulatory bodies, where

applicable and required under applicable law. In the event criminal activity is known to have occurred or suspected to have occurred SDL will notify the appropriate Police Authorities.

SDL reserves the right to delay notification under any contractual agreement in the case where law enforcement is investigating the breach, or when the delay is necessary to restore the reasonable integrity of the information system.

4.10. Data processing agreement

For all Customers controlling data of European Economic Area, UK and Swiss citizens, SDL can offer a data processing agreement with applicable Standard Contractual Clauses and/or other transfer agreements.

4.11. RWS ISO Accreditation for SAAS activity:

At the date of the latest version of this document, RWS's accreditation covers the following:

ISO 27001:2013

Locations:

- Maidenhead
- Sheffield
- Bangalore
- Cluj

Products: Translation Productivity tools and RWS hosted solutions for Translation Management, Knowledge Delivery, Digital Experience and Language Cloud.

RWS is constantly reviewing the scope of the ISO accreditation adding further locations and products over time.

4.12. RWS SOC 2 Type 2 Accreditation for Cloud Hosting:

SOC 2 is an attestation report provided by a service auditor to provide controls assurance of RWS Cloud Operations operational processes relevant to trust service categories of security, availability and confidentiality. Annually, RWS undergoes an audit of its controls for all SAAS products and is certified as compliant. A SOC 2 report can be provided upon request with a signed NDA.

Schedule 1: Products and Personal Data Processing

Software	Processes Personal Data for Data Controller
RWS Tridion Sites	Personal Data could be stored in Web at the Customer's option, as contractually agreed.
RWS ManTra	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS Language Cloud, Trados Enterprise & RWS Trados Live	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS TMS	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS WorldServer	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS Trados Groupshare	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS Tridion Docs	It is not anticipated Personal Data will be processed.
RWS MultiTerm	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS Dynamic eXperience Delivery (DXD)	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS Secure Translation (VDI)	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS MultiTrans TMS	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS DataDrop	Processing of Personal Data is possible at the Customer's option, as contractually agreed.
RWS MT LanguageWeaver Edge	Processing of Personal Data is possible at the Customer's option, as contractually agreed.

Schedule 2: Locations and 3rd party service provider

Data Centre Location	Service Provider	Certification	Software	Offsite Backup Provider
Region EU Region JP Region US Region UK Region Canada	Amazon Web Services (AWS)	ISO 27001 SSAE16 SOC 1, 2 and 3 EU-US Privacy Shield Protected B	• RWS Tridion Sites • RWS Tridion Docs • RWS GroupShare • RWS TMS • RWS MultiTrans TMS • RWS DataDrop • RWS Secure Translation (VDI) • RWS Dynamic eXperience Delivery (DXD) • RWS MT Edge	Amazon
Region Beijing China Region Frankfurt	Alibaba	ISO 27001 SOC 2	• RWS Tridion Sites • RWS MultiTrans TMS • RWS Groupshare	Alibaba