SDL Privacy Policy
Cloud Services

Software-As-A-Service Products

Version 30-10-2014

SDL plc

Globe House
Clivemont Road, Maidenhead
SL6 7DY England
www.sdl.com

Summary

This privacy policy is an appendix to the Master Subscription Services Agreement to give customers insight in security measures SDL has in place to assure confidentiality, integrity and availability of customers information. The policy is based on industry best practices, and fulfills an important role in executing the European Data Protection Directive.

In this policy a Data Processing Agreement template is included, for our European Customers for which SDL processes information.

Table of contents

Version Management

This document can be retrieved from the author.

Version history

Version	Date	Author	Distribution
0.0 initial document	06-08-2014	Jeroen Aijtink	SDL Internal
0.1	08-08-2014	Jeroen Aijtink	SDL Internal
0.2	21-08-2014	Jeroen Aijtink	SDL Internal
0.9	15-09-2014	Jeroen Aijtink	SDL Internal
1.0	03-10-2014	Jeroen Aijtink	SDL Internal
1.1	30-10-2014	Jonathan Slaughter	SDL Internal

Approval

This document requires the following approval:

Name	Department	Title/Position
Dennis van der Veeke	DevOps	CTO
Jan Wiersma	Cloud Services	VP Cloud services
Harpreet Sagoo	Legal – Maidenhead	VP Legal & Contracts

1. Introduction

This Privacy Policy is written in addition to the Master Subscription Services Agreement for hosted SAAS-products, to give customers some insights in the security measures SDL has in place to protect their information. This policy originated from the Cloud Security Alliance whitepaper on a privacy agreement within the European Union.

Details on how SDL employees handle (personal) customer information are found in security policies and procedures. Those documents are classified as Information Classification Level 2 – SDL Confidential, and therefore, only available for SDL representatives.

Beside this privacy policy, information about collecting, processing or handling personal information can be found on SDL's corporate website (www.sdl.com/aboutus/privacypolicy.html).

2. Privacy Policy

This Privacy Policy is used as appendix on the Master Subscription Services Agreement for hosted SAAS-products. The policy describes the level of privacy and data protection SDL undertakes to maintain security during data processing. This policy covers all hosted products in the SDL Customer Experience Cloud. In terms of the DPD, SDL operates as processor of data, for which customer is the controller.

This policy shall be deemed to take effect from the Effective Date and shall continue in full force and effect until the termination of the Agreement or return of all information assets to the Licensee has occurred.

2.1. Definitions

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

DPD	Means the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995;
DPA	Means data processing agreement as defined in the DPD;
Personal data	Means personal data as defined in the DPD that the Processor (SDL) processes on behalf of Controller (customer) in connection with the Master Subscription Services Agreement for hosted SAAS-products
Liscensee	The customer who purchases hosted services from SDL, listed on the executed Master Service Agreement
Data subject	Means any identified or identifiable natural person as defined in the DPD
Data controller	Organization that has the authority to decide how and why personal information is to be processed
Data processor	Individual or organization, often a third-party outsourcing service, that processes data on behalf of the data controller

2.2. Scope and Categories

This policy describes the collection, processing and use of personal data in hosted products by processor (SDL). The hosted products process personal data on behalf of the controller; however, SDL shall not use the personal data for any other purpose than those agreed to with the controller. The table below describes services and stored information.

Service	Stored personal data for controller
SDLWeb	Personal data could be stored inside SDL Web and is the responsibility of controller (Licensee).
SDL Fredhopper	Fredhopper does not contain personal data.
SDL Customer Journey Analytics	Personal data is, after collection, stored inside this service.

Service	Stored personal data for controller
SDL Media Manager	Media Manager does not contain personal data. Processing of personal data is possible within this service.
SDL Campaigns	Personal data (like demographic and transaction) is stored and processed inside these services. Processing of personal data is conducted on behalf of controllers request.
SDL BeGlobal	SDL BeGlobal does not store personal data. Processing of personal data is possible within this service.
SDL Language Cloud	SDL Language Cloud does not store personal data. Processing of personal data is possible within this service.
SDL Translation Management Server and SDL World Server	TMS and/or WS do not store personal data. Processing of personal data is possible within these services.
SDL Enterprise Translation Server	SDL ETS does not store personal data. Processing of personal data is possible within this service.
SDL Groupshare	SDL Groupshare does not store personal data. Processing of personal data is possible within this service.
SDL Live Content	SDL Live Content does not store personal data.
SDL MultiTerm	SDL MultiTerm does not store personal data.
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 not be shared outside SDL.	

Prohibited data: the following information categories are not allowed storage on any of SDL's SAAS-products:

- Gambling (unless explicit approval has been provided by SDL);
- Pornography;
- Illegal or Terrorist activity;
- Medical records;
- Payment card.

Locations and 3rd party service provider

SDL may use 3rd party service providers for its infrastructure and platform services. All SDL service providers follow highest industry standards (for example certified on ISO27001 or SSAE 16 SOC 2) on physical and information security. Table below describes subcontractors used for hosting services and their datacenter locations for personal data storage. Backups of databases containing personal information are stored in a backup location for business continuity purposes.

DC Location	Service Provider	Certification	Services
San Jose	NTT	ISO27001	• SDL Enterprise Translation Server • SDL Groupshare

DC Location	Service Provider	Certification	Services
(USA)		SSAE 16 SOC 2 Safe Harbor	• SDL Live Content • SDL MultiTerm • SDL Translation Management System • SDL Smart Target • SDL World Server
Slough (UK)	NTT	ISO27001	• SDL Groupshare • SDL MultiTerm • SDL Translation Management System • SDL Live Content
Bristol (UK)	Kingston Communications	ISO27001	• SDL Campaigns
Denver CO (USA)	Fortrust	SSAE16 SOC	• SDL Campaigns • SDM Customer Journey Analytics
Irvine CA (USA)	Latisys	SSAE16 SOC 2 and 3 Safe Harbor	• SDL BeGlobal • SDL Language Cloud
Sydney (AUS)	NTT	ISO27001	• SDL Campaigns
Region EU Region JP Region US	Amazon	ISO27001 SSAE16 SOC 1, 2 and 3 Safe Harbor	• SDL Web • SDL Fredhopper • SDL Media Manager
	Akamai	Safe Harbor	• SDL Media Manager

Services generate log-information, which is stored and processed at the same datacenter as the service is running.

SDL employees do all application and system administration. As part of managed services delivery, employees may process personal data on behalf of the customer (Controller).

2.3. Data transfers

Offsite backups, where applicable are transferred between different SDL datacenters. Data is not transferred or shared between different SDL customers.

SDL Plc. complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. SDL

Plc has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement.

Within 30 days of termination of the contract SDL will securely delete controller's information. When agreed SDL can hand over personal data to controller. Afterwards personal data will be securely deleted according to our policies.

SDL will inform controller in case of law enforcement access to personal data is requested. When it's prohibited to inform controller directly, SDL will inform controller afterwards. Information is only provided after presenting court documents to SDL's legal department. Requested information is handed over directly to the law enforcement agency.

2.4. Data security

For security of personal data a layered architecture is implemented which facilitates different platform, infrastructure, and/or application layers. For platforms and infrastructure, SDL uses IAAS and PAAS services from NTT, Amazon, Akamai, Latisys, KCOM and/or Fortrust. These companies comply with highest industry standards[1] on both information and physical security. The applications are offered as a service and will potentially collect, process and use personal data. The following paragraphs give customers an overview of security measures.

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) is checked by firewalls.

All communication between end-users and services is secured with encrypted communication. Independent and trusted 3rd party digital certificates are used on web available 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.

System administrators follow policies and guidelines when administering systems containing personal data. These policies are part of ISMS and updated regularly. As part of ISO 27001 certification controls are implemented in certain parts of the organization. ITIL processes are implemented within the cloud operations department for incident, change and release management.

[1] This can be ISO27001 and/or SSAE 16 SOC2.

Managed services department

As a part of managed services, SDL employees can access personal and customer data. Only the Cloud Applications & Production Services department can perform these tasks. Employees receive additional training on handling personal and/or customer data. Processing of any personal data is performed on behalf of the customer (controller) as described in a managed service agreement.

Privacy and security awareness within Cloud Services

Within the Cloud Services Department, all employees receive both 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 executed in addition to the annual general security awareness training. Attendance and effectiveness is monitored and tracked for auditability. Attendance of those trainings is mandatory.

An information security plan is created and updated by the Information Security Officer within the Cloud Services department. The knowledge of the Information Security Officer is updated via mandatory trainings and certification. For example, the Information Security Officer is CISSP certified.

To assure confidentiality and integrity, SDL has defined the Information Privacy Officer role within the Cloud Services department. The privacy officer will control for proper handling if privacy sensitive information within the SAAS-products. As with security, and privacy program is implemented and maintained by the Information Privacy Officer. The knowledge of the Information Privacy Officer is also updated via mandatory trainings and certification, including CIPP certification.

Both roles work closely to ensure the confidentiality, integrity and availability of information.

2.5. Monitoring

Rectification, deletion and blocking of data: Upon instruction by the Customer (Controller), SDL shall correct, rectify or block the personal data. Any request from a data subject directly to SDL, shall be directed to customer.

Please note, that where the removal of such data directly prohibits the contractually agreed upon activities between SDL and customer; requires signifanct costs; or puts other individual personal data at undue risk for exposure, SDL retains the right to deny the request. A formal description of reasoning and any appeals process is supplied upon denials.

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

SDL Plc Globe House
Clivemont Road
Maidenhead
SL6 7DY England

Tel: +44 (0) 1628 760610
Fax: +44 (0) 1628 760611
Email: **privacy@sdl.com**

2.6. 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 controller via e-mail as soon as possible after detection of a (suspected) personal data breach. Additionally, SDL notifies appropriate jurisdictional bodies, where applicalble.

SDL reserves the right to delay notification beyond 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.

2.7. Data processing agreement

For all customers handling data of European citizens, SDL can offer a data processing agreement. This agreement details the type and storage location of information SDL processes for the customer.

About SDL

SDL (LSE: SDL) allows companies to optimize their customers' experience across the entire buyer journey. Through its web content management, analytics, social intelligence, campaign management and translation services, SDL helps organizations leverage data-driven insights to understand what their customers want, orchestrate relevant content and communications, and deliver engaging and contextual experiences across languages, cultures, channels and devices.

SDL has over 1,500 enterprise customers, over 400 partners and a global infrastructure of 70 offices in 38 countries. We also work with 72 of the top 100 global brands.