SDL Inc. EU and UK-US Privacy Shield Notice

Policy version: 2.0

Effective Date: 31 January 2019

The SDL Group of companies is an international commercial organization which due to the nature of modern business administration and due to the services it provides to its customers will transfer Personal Data between entities within the SDL Group. This Policy covers the transfer and processing of personal data between the European Economic Area ("EEA"), the United Kingdom and the United States. It sets out the conditions which apply to SDL Inc. and its U.S. subsidiaries and affiliates when they receive and process Personal Data from SDL UK Entities, SDL EEA Entities, Customers of such entities, Employees of such entities and from Customers of SDL Inc. in the EEA and UK and their customers in the EEA and UK.

SDL Inc and its U.S. subsidiaries and affiliates (collectively, "SDL") respect your concerns about privacy. SDL has certified that it complies with the EU-US Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, storage, use, retention, transfer and other processing of Personal Data and Customers' Personal Data transferred from the EEA and the United Kingdom to the United States in reliance on Privacy Shield in connection with the activities described below.

SDL Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

SDL's EU-US Privacy Shield certification can be found at
https://www.privacyshield.gov/PS-Application

For more information about the EU-US Privacy Shield principles, please visit
https://www.privacyshield.gov/

This Policy outlines SDL's general policy and practices for implementing the EU-US Privacy Shield privacy principles for Personal Data and Customers' Personal Data, as applicable.

For purposes of this policy:

"Consumer" means any natural person who is located in the EEA and UK, but excludes any individual acting in his or her capacity as an Employee or who is a Representative.

"Customer" means any EEA entity that registers for or purchases products or services from any SDL company.

"Customers' Personal Data" means any information that (i) is recorded in any form, (ii) relates to an identified or identifiable individual who is located in the EEA or UK, and (iii) SDL receives in the U.S. on behalf of its Customers.

"Employee" means any current, former or prospective employee of SDL EEA Entities who is located in the EEA or SDL UK Entities who is located in the UK. For purposes of this Policy, "Employee" includes any temporary employee, intern, other non-permanent employee,

contractor or consultant of SDL EEA Entities who is located in the EEA or SDL UK Entities who is located in the UK.

"Personal Data" means any data about an identified or identifiable individual that is within the scope of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data or UK Data Protection Act 2018, including Sensitive Personal Data, that (i) is transferred to SDL in the U.S. from the EEA or UK, (ii) relates to an identified or identifiable Consumer, Employee or Representative, (iii) can be linked to that Consumer, Employee or Representative, and (iv) is recorded in any form.

"Representative" means any current, former or prospective representative of any Customer or Vendor, and who is located in the EEA or UK.

"SDL EEA Entities" means legal entities trading in the European Economic Area (EEA), these are subject to change over time; a full list can be obtained from privacy@sdl.com.

"SDL UK Entities" means legal entities trading in the United Kingdom these are subject to change over time; a full list can be obtained from privacy@sdl.com.

"Sensitive Personal Data" means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by an individual or the disposal of such proceedings, or the sentence of any court in such proceedings.

"U.S. subsidiaries and affiliates" means legal entities trading in the United States, these are subject to change over time; a full list can be obtained from privacy@sdl.com.

"Vendor" means any supplier, vendor or other third party located in the EEA or UK that provides services or products to SDL EEA Entities or SDL UK Entities.

For more information about SDL's processing of Personal Data collected on the following SDL websites: www.sdl.com, www.sdltrados.com, appstore.sdl.com, community.sdl.com, languagecloud.sdl.com, info.sdl.com, oos.sdl.com, blog.sdltrados.com, blog.sdl.com, www.freetranslation.com and www.xopus.com (the "Sites"), please visit the applicable SDL online privacy policies which appear at the bottom of each Sites home page.

Notice

Through this Privacy Shield Policy, SDL notifies Consumers, Employees and Representatives about the purposes for which SDL collects and uses their Personal Data, the types of third parties to whom SDL discloses the Personal Data, the choices Consumers, Employees and Representatives have for limiting the use and disclosure of their Personal Data and how to contact SDL about the company's practices concerning Personal Data. Information regarding SDL's Employee Personal Data practices is contained in the SDL HR Privacy and Data Protection Policy (Europe and UK) which is available on SDL's intranet (HR pages) or from the local human resources representative for each SDL EEA Entity.

SDL's practices regarding the collection, storage, use, transfer, and other processing of Personal Data and Customers' Personal Data comply, as appropriate, with the Privacy Shield Principles of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access and recourse, enforcement and liability.

How SDL Obtains Personal Data and Customers' Personal Data and the Purposes for which it is collected

This is described for the following classes of data subjects:

1. Consumers and Representatives

SDL obtains certain Personal Data, such as contact information, directly from these classes of data subjects. This collection occurs, for example, when a Consumer visits one of the Sites and provides Personal Data through such Site. SDL obtains Personal Data associated with Representatives, such as contact information, for the purposes of providing its products and services to Customers, and administering and managing its relationships with Customers and Vendors.

2. Customers

SDL obtains Customers' Personal Data in connection with providing:

(i) hosted software-as-a- service (SAAS) products to its Customers (including, without limitation, its web content management, analytics, social intelligence, campaign management and translation products);
(ii) on-premise software products licensed to a Customer for use on their own premises (including, without limitation, translation products) through provision of professional services;
(iii) professional translation services; and
(iv) Customer support services related to the SAAS and on-premise software products, and professional translation services. In connection with the activities described in (i) through (iv), SDL acts as a service provider to its Customers and pursuant to their instructions.

SDL obtains above Personal Data for the purposes of providing its products and services to Customers, and administering and managing its relationships with Customers.

3. Employees

SDL obtains Personal Data about its Employees for the purposes of carrying out and supporting administrative and human resources functions and activities, including:

(i) recruiting and hiring job applicants;
(ii) managing Employee performance;
(iii) determining Employee compensation;
(iv) for other general human resources purposes; and
(v) for information technology-related purposes (such as data storage, application hosting and maintenance; email; telephony and network connectivity; data back-up and restoration; disaster recovery and business continuity planning; and other

technical, organizational and administrative functions).

In addition, SDL obtains Personal Data about Employees' emergency contacts, dependents and beneficiaries to the extent our Employees provide the information to us. We process this information to comply with our legal obligations and for internal administrative purposes.

Choice

SDL offers Consumers, Employees and Representatives the opportunity to choose whether SDL may (i) disclose their Personal Data to third parties or (ii) use their Personal Data for purposes which are materially different from the purposes for which it was originally collected or subsequently authorized by the Consumer, Employee or Representative.

However, this choice is not available in these circumstances:

i. When SDL acts as a service provider, under a written contract, for its Customers and so is acting as an agent to perform task(s) on behalf of and under the instructions of the Customers.

ii. When SDL discloses the Personal Data to a third party which acts solely as an agent for SDL to perform task(s) on behalf of and under the instructions of SDL. SDL will always enter into an appropriate written contract with the agent.

When SDL processes Sensitive Personal Data, including any sensitive personal information received from a third party where the third party identifies and treats it as sensitive, SDL requires affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt in choice.

SDL may disclose Personal Data and Customers' Personal Data without offering an opportunity to opt out:

(i) if it is required to do so by law or legal process;
(ii) to law enforcement or other government authorities;
(iii) for purposes of assessing or monitoring compliance with legal and regulatory obligations or legitimate accounting activities in respect of necessary audits, or accreditation to standards or due diligence reviews for purposes of potential mergers or takeovers; and
(iv) when SDL believes disclosure is necessary to prevent physical harm or financial loss, or in connection with an investigation of suspected or actual illegal activity.

SDL also reserves the right to transfer Personal Data and Customers' Personal Data in the event it sells or transfers all or a portion of its business or assets (including in the event of a reorganization, dissolution or liquidation). SDL uses Personal Data and Customers' Personal Data only for the purposes indicated in this Policy unless it has a legal basis, such as consent, to use it for other purposes. To the extent required by law, SDL obtains prior opt-in consent at the time of collection for the processing of (i) Personal Data for marketing purposes and (ii) Sensitive Personal Data.

Onward Transfer of Personal Data

SDL may disclose Personal Data and Customers' Personal Data with third parties which act as agents for SDL as indicated in the "Choice" section above. Agents will include but are not limited to Data Centre providers for storage of data and providers of software as a service in the sales management process. The Personal Data will only be processed for the limited and specified purposes consistent with the consent provided by the data subject and that the third party will provide the same level of protection as SDL.

SDL may disclose Personal Data and Customers' Personal Data with third parties acting as a Data Controller. SDL will comply with the Privacy Shield Notice and Choice Principles. SDL will enter into a contract with the third-party Data Controller that provides that such Personal Data will only be processed for the limited and specified purposes consistent with the consent provided by the data subject and that the third party will provide the same level of protection as SDL.

When SDL discloses Personal Data and Customers' Personal Data to a third party which is subject to the European Union Data Protection Directive 95/46 or an adequacy finding under the Directive that shall be considered adequate protection.

If disclosure to third parties takes place SDL will remain liable for the processing of the Personal Data while undertaken by its agents only. SDL shall remain liable under the Principles if its agent processes such Personal Data in a manner inconsistent with the Principles, unless SDL proves that it is not responsible for the event giving rise to the damage.

Security

SDL takes reasonable and appropriate precautions to protect Personal Data and Customers' Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction. SDL has a data deletion policy and all data is deleted in accordance with the policy which can be obtained from privacy@sdl.com.

Data Integrity

SDL takes reasonable steps to ensure that the Personal Data and Customers' Personal Data it processes are:

(i) relevant for the authorized purposes for which they are to be used;
(ii) reliable for their intended use; and
(iii) accurate, complete and current.

In this regard, SDL depends on Consumers, Employees and Representatives and, with respect to Customers' Personal Data, on Customers, to update and correct Personal Data and/or respond to requests of SDL to update Personal Data to the extent necessary for the purposes for which the information was collected or subsequently authorized by the relevant data subject. Consumers, Employees and Representatives, and Customers, as appropriate, may contact SDL as indicated below to request that SDL update or correct relevant information.

Access

Where appropriate or required by applicable law, SDL provides Consumers, Employees and Representatives with reasonable access to the Personal Data SDL maintains about them. SDL also provides a reasonable opportunity for Consumers, Employees and Representatives to correct, amend or delete that information where it is inaccurate, as appropriate or where it has been processed in violation of the Principles. SDL may limit or deny access to Personal Data where providing such access is unreasonably burdensome or the expense of providing access would be disproportionate to the risks to the Data Subject's privacy in the case in question, or where the rights of persons other than the Data Subject would be violated. The right to access Personal Data also may be limited in some circumstances by local law requirements. Consumers, Employees and Representatives may request access to their Personal Data by contacting SDL as indicated below.

With respect to Customers' Personal Data, SDL acts as a service provider for its Customers. Therefore in order to preserve the accuracy of the Personal Data the relevant Customer ought to be contacted to manage the correction, amendment or deletion of Personal Data. Consequently the relevant Customers are responsible for providing Data Subjects with access to their information and the right to correct, amend or delete the information where it is inaccurate. When an individual is unable to contact the appropriate Customer, or does not obtain a response from such Customer, SDL will provide reasonable assistance in forwarding the individual's request to the relevant Customer, which will include providing the Customer with the Data Subject's Personal Data.

Annual Review

SDL has established procedures for periodically verifying implementation of and compliance with the Privacy Shield principles. SDL conducts an annual self-assessment of its practices to verify that the attestations and assertions SDL makes about its privacy practices are true and that its privacy practices have been implemented as represented.

Recourse and Enforcement

Consumers, Employees and Representatives may file a complaint concerning SDL's processing of their Personal Data at privacy@sdl.com. SDL will respond promptly, and in any event in no more than 45 days, to complaints and endeavor to investigate and resolve complaints expeditiously, at no cost to the Data Subject, by reference to the Privacy Shield Principles and provide compensation by way of damages where the applicable law provides. SDL will take reasonable and appropriate steps to remedy any issues arising out of a failure to comply with the Privacy Shield principles.

With respect to Customers' Personal Data, SDL acts as a service provider for its Customers, consequently the ultimate control of the Personal Data remains with the Customer. Therefore Data Subjects should submit complaints concerning the processing of their information to the

relevant Customer, in accordance with the Customer's dispute resolution process. SDL does require the Data Subject to identify the Customer in order for SDL to identify the correct Personal Data. SDL will participate in this process at the request of the Customer or the Data Subject and Data Subject can use the SDL complaint process explained below.

If a Consumer or Representative complaint cannot be resolved through SDL's internal processes, or a complaint related to Customers' Personal Data cannot be resolved through the relevant Customer's dispute resolution process, the unresolved complaint may be referred to the following:

a) the relevant EU or UK state or national data protection authority. SDL commits to cooperate in investigations by and to comply with the advice of competent EU or UK authorities in such cases which can be implemented at proportionate cost.

b) A Data Subject may refer the complaint to the U.S. Federal Trade Commission, which has Privacy Shield investigatory and enforcement jurisdiction over SDL.

c) All unresolved complaints can be referred to binding arbitration as provided in Annex 1.

How to Contact SDL

To contact SDL with questions or concerns about this Privacy Shield Privacy Policy or SDL's practices concerning Personal Data or Customers' Personal Data the **Data Privacy Officer** ought to be contacted:

In the USA write to:	In the EEA write to:
SDL Inc The Legal Department 101 Edgewater Drive, Suite 210 Wakefield, MA 01880 Email: privacy@sdl.com	SDL PLC The Legal Department New Globe House, Vanwall Road, Vanwall Business Park, Maidenhead, Berkshire, SL6 4UB Email: privacy@sdl.com

ANNEX I

This Annex I provides the terms under which Privacy Shield organizations are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain "residual" claims as to data covered by the EU-U.S. Privacy Shield. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of claimed violations of the Principles not resolved by any of the other Privacy Shield mechanisms, if any.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles[1] or with respect to an allegation about the adequacy of the Privacy Shield.

[1] Section I.5 of the Principles.

B. Available Remedies

Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in Section III.11(d)(i) of the Principles; (2) make use of the independent recourse mechanism under the Principles, which is at no cost to the individual; and (3) raise the issue through their Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual.

This arbitration option may not be invoked if the individual's same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties.

In addition, this option may not be invoked if an EU Data Protection Authority (1) has authority under Sections III.5 or III.9 of the Principles; or (2) has the authority to resolve the claimed violation directly with the organization. A DPA's authority to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes

the option to seek relief for the same claimed violation in another forum, except that if nonmonetary equitable relief does not fully remedy the claimed violation, the individual's invocation
of arbitration will not preclude a claim for damages that is otherwise available in the courts.

E. Review and Enforcement

Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.[2] Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the Privacy Shield organization.

[2] Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention")]." 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select the arbitrators from the list of arbitrators discussed below.

Consistent with applicable law, the U.S. Department of Commerce and the European Commission will develop a list of at least 20 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

(1) will remain on the list for a period of 3 years, absent exceptional circumstances or for cause, renewable for one additional period of 3 years;

(2) shall not be subject to any instructions from, or be affiliated with, either party, or any Privacy Shield organization, or the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and

(3) must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in EU data protection law.

G. Arbitration Procedures

Consistent with applicable law, within 6 months from the adoption of the adequacy decision, the Department of Commerce and the European Commission will agree to adopt an existing, well established set of U.S. arbitral procedures (such as AAA or JAMS) to govern proceedings before the Privacy Shield Panel, subject to each of the following considerations:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a "Notice" to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual's same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, EU DPAs may provide assistance in the preparation only of the Notice but EU DPAs may not have access to discovery or any other materials related to these arbitrations.
5. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.
6. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing as well as translation of arbitral materials will be provided at no cost to the individual, unless the panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
9. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations. Subject to applicable law, the Department of Commerce will facilitate the establishment of a fund, into which Privacy Shield organizations will be required to pay an annual contribution, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts ("caps"), in consultation with the European Commission. The fund will be managed by a third party, which will report regularly on the operations of the fund. At the annual review, the Department of Commerce and European Commission will review the operation of the fund, including the need to adjust the amount of the contributions or of the caps, and will consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the mutual understanding that there will be no excessive financial burden imposed on Privacy Shield organizations. Attorney's fees are not covered by this provision or any fund under this provision.