Brand Management
& Productivity
Tools for Microsoft Office

Skabelon Design

DATA PROCESSING AGREEMENT

BETWEEN

SkabelonDesign A/S

Danish company registration No. (CVR): DK-35679529
Wilders Plads 15-A
DK-1403 Copenhagen
Denmark

(the "Data Processor")

AND

Each individual SkabelonDesign Customer that SkabelonDesign A/S processes data for and that has not otherwise entered into a valid data processor agreement with SkabelonDesign A/S

(the "Data Controller")

(hereinafter referred to individually as a "Party" or together as the "Parties")

Contents

1. Introduction

This Data Processing Agreement ("DPA") specifies the Parties' data protection obligations which arise from the Data Processor's processing of personal data on behalf of the Data Controller under the quote, service agreement or other agreement between the Parties ("the Agreement").

The DPA is adopted as an appendix to the Agreement. In the event that any provision of this DPA is inconsistent with any term(s) of the Agreement, the DPA will prevail.

2. Purpose, Scope and responsibilities

1. The Data Processor shall only process personal data in accordance with the terms of this DPA.

2. The Data Processor shall process personal data for the limited purpose of performing the obligations set out under the Agreement.

3. Data processing by the Data Processor shall include such actions as may be specified in the Agreement.

4. The term of this DPA shall continue until the latter of the following; the termination of the Agreement, or the date at which the Data Processor ceases to process personal data for the Data Controller.

3. Data flow

1. The Data Processor is a software development company, assigned by the Data Controller to make available to the Data Controller software as a service for supporting the creation of business documents. The content of this DPA reflects the limited amount of personal data the Data Processor handles for the Data Controller.

2. A general list of the data processed by the Data Processor can at every given time be required upon request to the Data Processor.

3. In no event will the data processed by the Data Processor include (examples are not exhaustive):
   - Personal data as set out in art. 7 or 8 in the Danish Personal Data Protection Act,
   - Personal data as set out in art. 9 or 10 in Regulation 2016/679 of 27 April 2016
   - Financial data (unless actively required by Data Controller),
   - Personal data regarding criminal offences, or
   - Data regarding persons' economy, taxes, debt, sick days, family relations, residential circumstances, car, personality tests.
   - The Data Processor's services data flow is described in Exhibit 1 (the "Data Flows"). This list may include services not licensed by the Data Controller. Services, which are not licensed by the Data Controller are not effective and does not process data for this tenant.

4. Obligations of Data Processor

The Data Processor warrants that the Data Processor will:

a) Comply with the Data Protection Legislation from time to time applicable to the Data Processor's obligations under the Agreement ("Data Protection Legislation"),

b) process any personal data transferred to or collected by the Data Processor only as a 'processor', as such terms are defined in the Data Protection Legislation, on behalf of the Data Controller,

c) implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the applicable Data Protection Legislation and ensure the protection of the rights of the data subjects,

d) ensure that Sub-processors undertakes to process personal data in accordance with the Data Protection Legislation,

e) taking into account the nature of the processing, assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights according to the Data Protection Legislation,

f) in relevant extent assist the Data Controller in ensuring compliance with the requirements for security of person data,

g) make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections to facilities under the control of the Data Processor, conducted by the controller or an auditor mandated by the controller.

5. Technical and organisational security measures

1. The Data Processor will implement and maintain throughout the term of the DPA and will procure its Sub-processors to implement and maintain through the term of the DPA, the appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction, loss, damage or alteration and against unauthorized disclosure, abuse or other processing in violation of the requirements of Data Protection Legislation.

2. The Data Processor will ensure that it and its Sub-processors involved in the processing of personal data at all times comply with the minimum data security requirements set out in *Exhibit 2*.

6. Personnel

1. The Data Processor will procure that any personnel of the Data Processor required to access personal data have committed themselves to the obligation of confidentiality set out in the Agreement or are under a statutory obligation of confidentiality.

2. The Data Processor will procure that all personnel of the Data Processor required to access personal data are informed of the confidential nature of the personal data and the security procedures applicable to the processing of or access to the personal data.

3. The Data Processor's personnel's undertaking to abide by such confidentiality requirements will continue after the end term of this DPA.

7. Additional responsibilities of the Data Processor

1. To the extent possible, the Data Processor will:

2. Notify the Data Controller without undue delay of any monitoring activities and measures undertaken by a supervisory authority pursuant to Data Protection Legislation, if such monitoring activities and measures pertains to the data processed under the Agreement;

3. Notify the Data Controller in writing within five (5) business days if it receives (i) a request from a data subject to have access to that person's personal data; or (ii) a complaint or request relating to the Data Controller's obligations under the Data Protection Legislation.

8. Sub-processors

1. The sub-processors approved at the signing of this DPA are listed in *Exhibit 3*.

2. The Data Processor is authorized to engage further or other sub-processors if deemed relevant or necessary by the Data Processor for the purpose of performing the Data Processor's obligations under the Agreement. In such case, the Data Processor will ensure to notify the Data Controller at least 30 days prior to the engagement of further or other sub-processors. The Data Controller may object to such new Sub-processor for justified reasons. In the case of justified objection, the Parties shall negotiate in good faith to find an alternative solution. If such alternative solution cannot be found and the Data Processor decides to proceed with such sub-processor, the Data Controller can terminate the Agreement with a notice of 30 days. Neither of the Parties shall be considered in breach of contract in the event of such termination;

3. Where the Data Processor sub-contracts its obligations, as described above, it shall do so only by way of a written agreement with the sub-processor which imposes the sub-processors to comply with the obligations of the Data Protection Legislation.

4. The Data Processor may only transfer personal data within the EU/EEA or within countries that have been recognized by the EU Commission to ensure an adequate level of data

protection. The Data Processor may not transfer data outside these countries without the prior written approval of the Data Controller. In the event such approval is granted, the Data Processor undertakes to comply with the requirements after the Data Protection Legislation for transfer out of the EU/EEA, e.g. by use of the Commission's model contracts, Privacy Shield Institute, consent from the data subjects or similar, to the extent applicable.

5. At the signing of this DPA, approval for transfer of personal data out of the EU/EEA, cf. section 8.4, has been given for transfer to the sub-contractors listed in *Exhibit 3*.

6. A list of the Sub-processors engaged by the Data Processor and a copy of the data processing agreement(s) between the Data Processor and the Sub-processors can at every given time be required either upon request to the Data Processor.

9. Obligations of the Data Controller

1. The Data Controller and the Data Processor will be separately responsible for conforming with the Data Protection Legislation as applicable to them.

2. The Data Controller will inform the Data Processor in writing without undue delay following the Data Controller's discovery of a failure to comply with Data Protection Legislation with respect to processing of personal data in accordance with this DPA.

10. Notification of data breach

1. The Data Processor shall without undue delay in writing notify the Data Controller in case of any identified or potential breach of personal data processed under the DPA.

2. The notification referred to in section 10.1. must, to the extent possible, contain:

   h) describe the nature of the personal data breach including where possible (e.g. loss, theft, copying), the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

   i) communicate the name and contact details of the person with the Data Processor where more information can be obtained,

   j) describe the likely consequences of the personal data breach, and

   k) describe the measures taken or proposed to be taken by the Data Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

11. Deletion of Personal Data

1. Following the end term or termination of the Agreement, the Data Processor will destroy all personal data processed for the Data Controller that is in the Data Processors

possession or control, unless requirements arising from the Data Protection Legislation requires storage of the personal data.

2. Upon the Data Controller's request, the Data Processor shall certify in writing the destruction of the personal data.

12. Signatures

Signed for and on behalf of the Data Processor

Date:

_____

Name: Jakob Bjersing

Title: CFO, SkabelonDesign A/S

Exhibit 1: Data Flow

This Exhibit 1 sets out the data flow between the Data Controller and the Data Processor under the DPA.

The Data Processor provides Software-as-a-Service solutions to support the Data Controller users in creation of business documents. These are:

1. On premise: On premise solutions, offering functionality in Software (e.g. MS Office) used by the Data Controller, without storing or processing data.

2. On premise – client: On premise solutions, which processes data client-side, by querying data available in the Data Controllers infrastructure when triggered by a Data Controller user's action. These data will never be stored or transferred outside of the infrastructure of the Data Controller.

3. On premise – hybrid: On premise solutions, which depends on additional data processing at #5, triggered by a Data Controller user's action. Transaction is logged to ensure continuous integrity of service for Data Controller.

4. Cloud: Running on #5, synchronizations of data between Data Controller systems. No data is stored post the synchronization.

5. Backend (License heartbeat & #3 & #4): Global and generic multi-tenant SaaS solutions, that are hosted by SkabelonDesign in the Microsoft Azure Cloud.

6. Documotor: Document Generation API as a Service (SaaS) that can run hosted in SkabelonDesign infrastructure, multi-tenant, or be deployed to your infrastructure using docker (Containers-as-a-Service), single tenant.

#1 and #2 consumed by the Data Controller users may perform a licensing heartbeat to #5, to prevent license overuse on an organizational level. This transaction stores anonymized data: the windows domain, global IP address and hashed windows user name, of the Data Controller user. Hashed user name and global IP address are persisted for a limited time (typically 30 days).

Regarding #5, solutions offering user configuration in the sense of a user-based web interface, utilizes a database with emails and hashed passwords for users in conjunction with storage of information required for Data Controller systems to perform #3 and #4, e.g. service credentials and API secrets.

#6, Documotor receives a data payload. This payload is streamed to the appropriate internal processor, i.e., Word/PowerPoint templating engine. Once the document has been processed it is returned to the requester.

The document is not persisted or recoverable. The client can store sample data for template configuration by enabling data recording. This will persist the latest payload until disabled and cleared by the client.

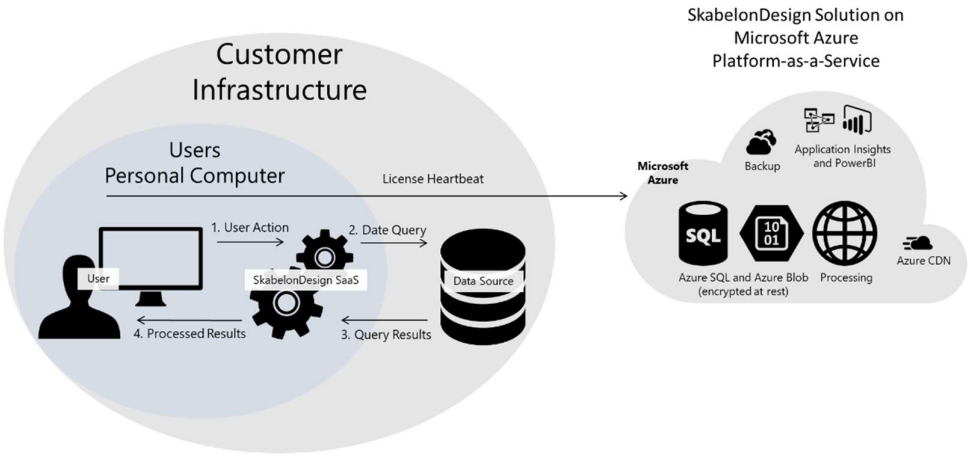
Templates based on pipelines can be configured to utilize external systems outside of SkabelonDesign.

All information is encrypted at rest and in transit.

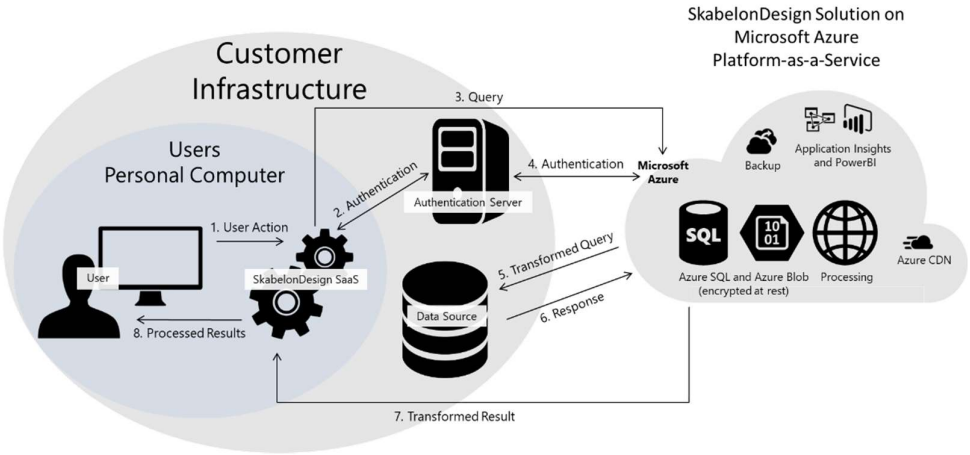
Referring to the above list, the Data Processor's data flow can be illustrated as follows:

1. On premise: No data flow, except license heartbeat (see #2), outside the application executing on the user's personal computer.

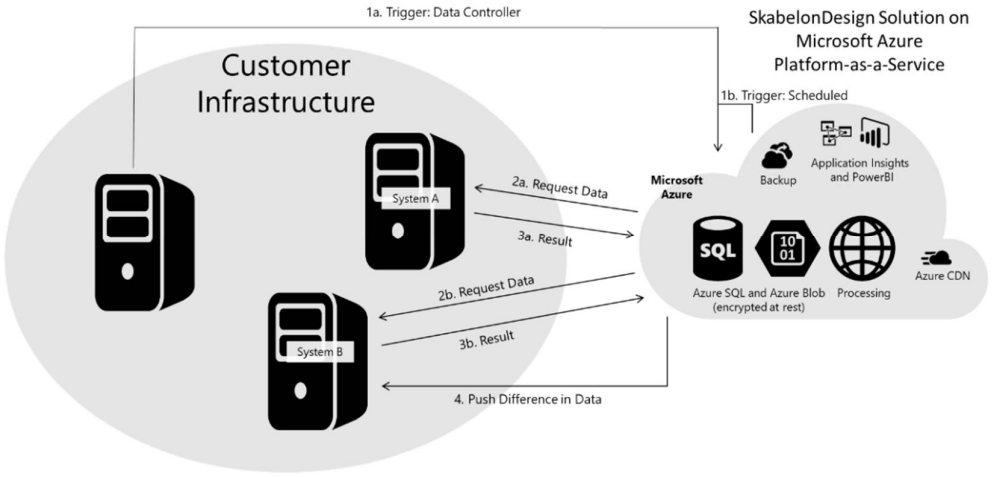
2. On premise – client:



3. On-premise – hybrid:



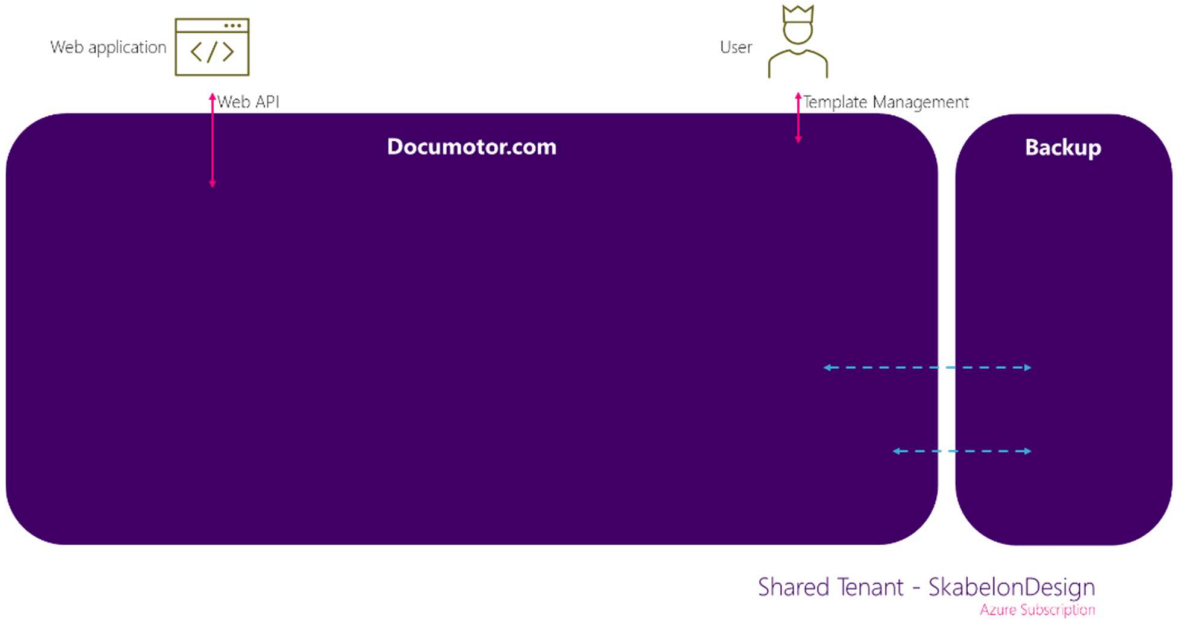
4. Cloud:



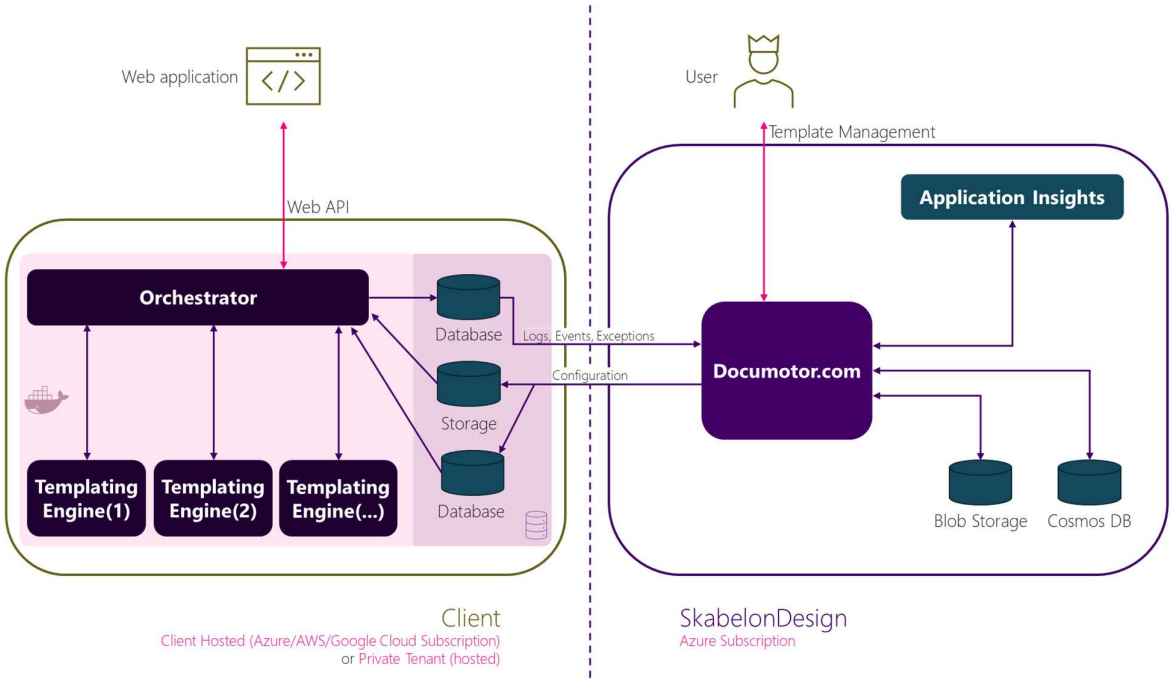
5. **Backend**: No illustration, described in #2, #3 and #4

6. **Documotor**:

    a. Cloud



b. Hybrid



Non-exhaustive list of generic products and services offered by Data Processor implementing the described types of solutions:

NAME	SOLUTION	NOTES
DOCUMOTOR	Documotor	
WORDENGINE	On premise	
PRESENTATIONENGINE	On premise	
PASTEXL	On premise	
CORPORATECHARTS	On premise	
CORPORATETABLES	On premise	
BRANDEDAGENDA	On premise	
LEGALTOOLS	On premise	
DOCUMENTWORKFLOW	On premise	
ACCESSIBILITYASSISTANT	On premise	
DOCUMENTDATAENGINE *BASIC COMPONENT FOR DATA BINDING IN OFFICE DOCUMENTS.*	On premise	Reads/writes data to/from office document on user PC.
OFFICEEXTENSIONS	On premise	

BASIC RIBBON AND TOOLS FOR OFFICE		
SHAREPOINT INTEGRATION FOR OFFICE	On premise	Reads/writes data to/from office document file using DocumentDataEngine.
FILEUPDATER	On premise – client	With self-hosted repository (data source).
DATAIMPORTER	On premise and On premise – client	Depending on configuration.
IMANAGE 9 AND 10 INTEGRATION FOR OFFICE	On premise – client	Through COM/Plugin integration in Office.
NETDOCUMENTS INTEGRATION FOR OFFICE	On premise – client	Through COM/Plugin integration in Office.
INTERACTION INTEGRATION FOR OFFICE	On premise – client	Through COM/Plugin integration in Office.
CV PARTNER INTEGRATION FOR OFFICE	On premise – client	
DYNAMICS CRM 365 INTEGRATION FOR OFFICE	On premise – hybrid	
SITECORE DAM INTEGRATION	Cloud	
OPENTEXT DAM INTEGRATION	Cloud	
GOOGLE DIRECTORY USER PHOTOS INTEGRATION	Cloud	
POWERFEED	Cloud	

Exhibit 2: Description of minimum Data security

The Data Processor will by itself, and shall ensure that all of its Sub-processors, at all times complies with the following minimum security requirements:

1. Availability

Data Processor has implemented the necessary security measures to ensure that data is available, e.g. through use of anti-virus and DDOS mitigation technologies etc.

2. Integrity

Data Processor has implemented the necessary security measures to ensure that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission, e.g. backup and authentication codes and signatures.

3. Confidentiality

Data Processor has implemented the necessary security measures to ensure the confidentiality of personal data, including, e.g. encryption technologies, training programs, authorization, contractual clauses etc.

4. Isolation (purpose limitation)

Data Processor has implemented the necessary procedures and controls to ensure that personal data is only accessed and used for legitimate purposes, e.g. through access management, division of roles and responsibilities etc.

5. Portability

Data Processor has ensured the portability of personal data, e.g. use of standardised or open data formats and interfaces.

6. Accountability

Data Processor has implemented the necessary technical and organisational measures to ensure accountability and traceability of the processing of personal data, e.g. through use of logging, self-auditing etc.

7. Physical security

Data Processor's business is cloud based and Data Processor does not use or provide physical storage of personal data. Such locations are provided by Sub-processors, as described in *Exhibit 3*.

Exhibit 3: Sub-Processors

This Exhibit 3 sets out the Data entailed by the Data Processor's and its Sub-processors' processing of personal data under the DPA.

Name	Personal data types	Description
Microsoft Azure Microsoft Ireland Operations Ltd, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Ireland Data processing at Azure Data Centers in Dublin, Ireland and Amsterdam, the Netherlands	• External Company IP Address • Work Company • Work e-mail address + other properties that the Data Controller configures SkabelonDesign to process e.g.: • Name • Work Title • Work Phones • Work Location • Photos • etc.	SkabelonDesign uses available features and services of Microsoft Azure to process and store the mentioned data types. The Microsoft Azure platform is trusted by US Military and 85% of Fortune 500 companies for core IT infrastructure. Microsoft data centres are state of the art with regards to security processes. Please refer to https://azure.microsoft.com/en-us/support/trust-center/ for more information on Microsoft Azure certifications, compliance and security processes. Microsoft is part of the EU/US Privacy Shield and complies with international data protection laws regarding transfers of customer data across borders.
Microsoft PowerBI Microsoft Ireland Operations Ltd, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Ireland Data processing at Azure Data Centers in Dublin, Ireland and Amsterdam, the Netherlands	• External Company IP address • Work company • Anonymized Work e-mail address	SkabelonDesign uses Microsoft PowerBI for usage and licensing statistics. PowerBI is a Microsoft Service running on Microsoft Azure. Please refer to https://www.microsoft.com/en-us/trustcenter/cloudservices/powerbi for more information on Microsoft PowerBI certifications, compliance and security processes. Microsoft is part of the EU/US Privacy Shield and complies with international data protection laws regarding transfers of customer data across borders.