Datenschutz konkret: Microsoft Cloud Lösungen im Gesundheitswesen

Daniel von Büren – Microsoft Schweiz

HAMILTON MEDICAL

About

- Daniel von Büren
- Technical Specialist Security & Compliance
- Ausbildung
  - Microsoft Senior Technical Leadership Program
  - Seminar Neues Datenschutzrecht
  - Security (CISSP, CEH, Security+)
  - Leadership & Management NDS
  - Betriebsingenieur HTL

Brückenbauer zwischen Datenschutz & Technologie

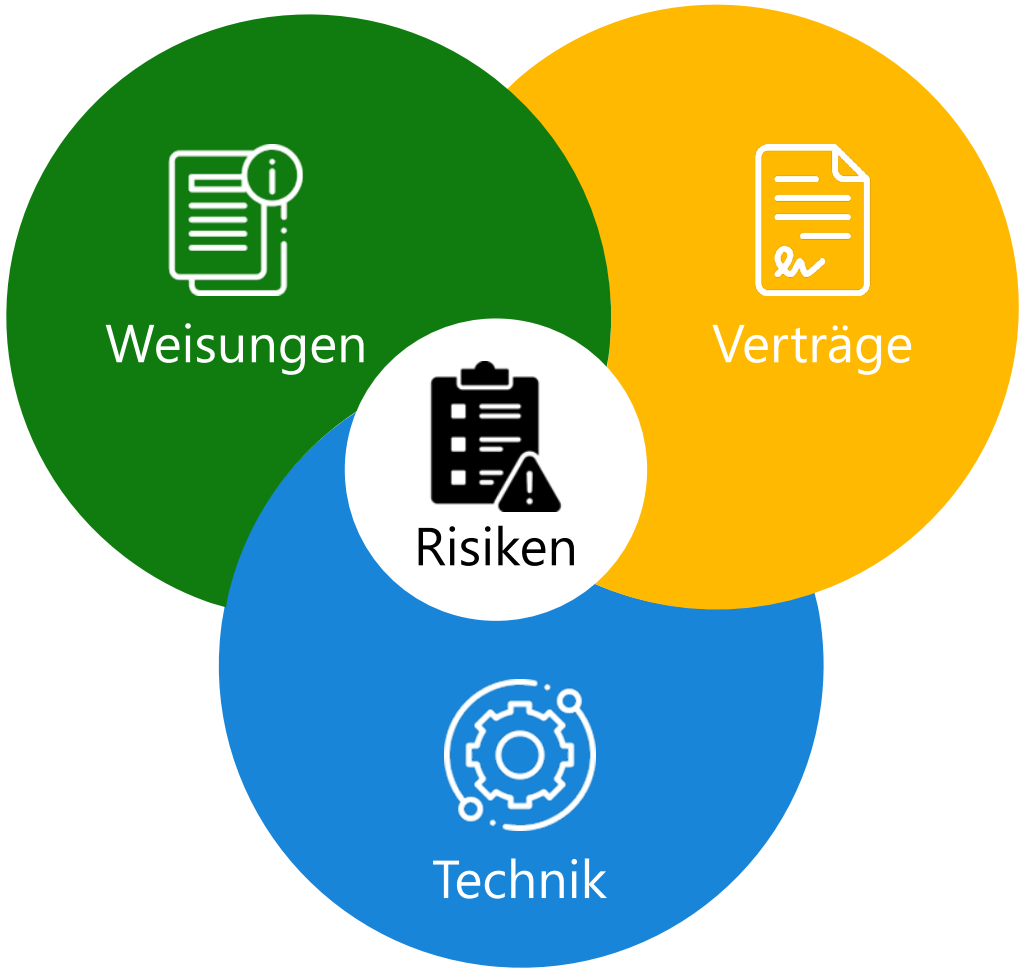
Wie kann Microsoft unterstützen?

Die Identifikation von potentiellen Risiken erfolgt durch die Rechtsberatung beim Kunden.

Microsoft kann anschliessend die gefundenen Risiken gemeinsam mit dem Kunden analysieren und Massnahmen aufzeigen, welche die Risiken minimieren können.

Die rechtliche Beurteilung der Wirksamkeit dieser Massnahmen obliegt schlussendlich beim Kunden.

Microsoft kann und darf keine rechtlichen Empfehlungen abgeben.



Ausgangslage

Hamilton Medical möchte Daten von ihren Beatmungs-geräten auf SharePoint verarbeiten, beziehungsweise speichern. Ihr externer Rechtsberater hat dazu folgende Bedenken:

"Der Schwachpunkt ist tatsächlich der potentielle Drittlandstransfer durch die Nutzung von Microsoft. Neben der Location EU/EWR bräuchte es noch eine vertragliche Garantie von Microsoft, dass es zu keiner Verarbeitung im Drittland kommt, beispielsweise durch Zugriff.

Der potentielle Behördenzugriff bereitet mir hier weniger Bauschmerzen. Es geht mehr um den tatsächlichen Zugriff, z.B. durch Microsoft-Personal in Indien und den USA."

Herausforderung I: Speicherort der Daten

Problemstellung

Aufgrund rechtlicher Anforderungen müssen Daten in bestimmten Regionen gespeichert werden (z.B. CH oder EU) und dürfen nicht ins (unsichere) Ausland transferiert werden.

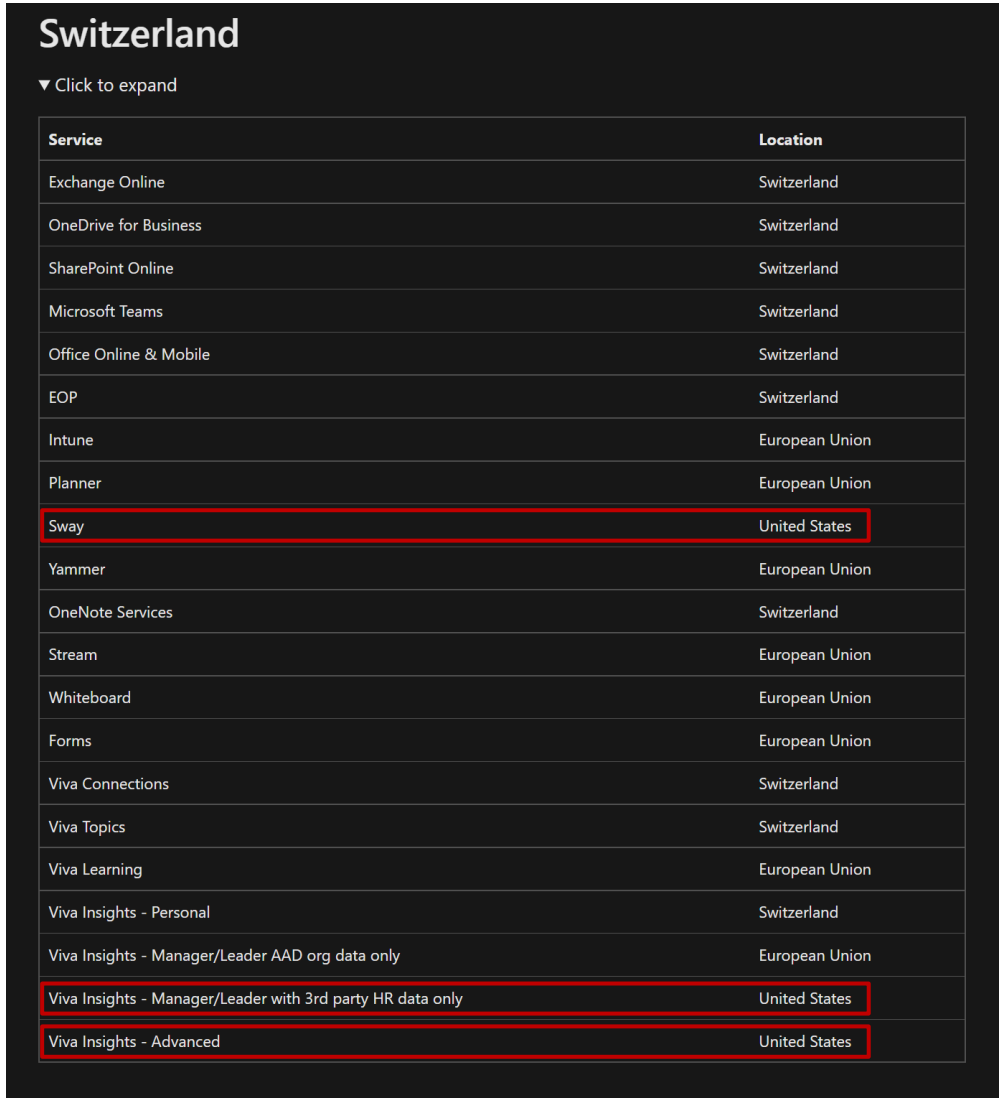
Lösungsansätze

Office 365

- Der Standort für Office 365 definiert den Standort wo Daten gespeichert werden (z.B. CH).
- Nicht alle Services werden aus der Schweiz erbracht!

Azure

- Der Standort kann pro Service definiert werden.
- Nicht alle Services sind überall verfügbar.



Switzerland

▼ Click to expand

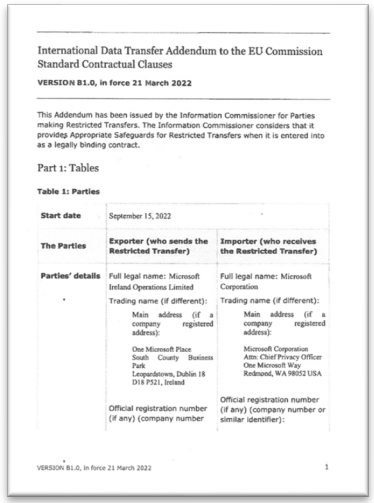
Service	Location
Exchange Online	Switzerland
OneDrive for Business	Switzerland
SharePoint Online	Switzerland
Microsoft Teams	Switzerland
Office Online & Mobile	Switzerland
EOP	Switzerland
Intune	European Union
Planner	European Union
Sway	United States
Yammer	European Union
OneNote Services	Switzerland
Stream	European Union
Whiteboard	European Union
Forms	European Union
Viva Connections	Switzerland
Viva Topics	Switzerland
Viva Learning	European Union
Viva Insights - Personal	Switzerland
Viva Insights - Manager/Leader AAD org data only	European Union
Viva Insights - Manager/Leader with 3rd party HR data only	United States
Viva Insights - Advanced	United States

Quelle: Where your Microsoft 365 customer data is stored

Herausforderung II: Zugriffe durch Microsoft

Problemstellung

Der Zugriff auf Kundendaten durch Microsoft (oder Unterauftragsverarbeiter) von ausserhalb Europas kann problematisch sein, da das Datenschutzniveau nicht mit dem der Schweiz übereinstimmt.



International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

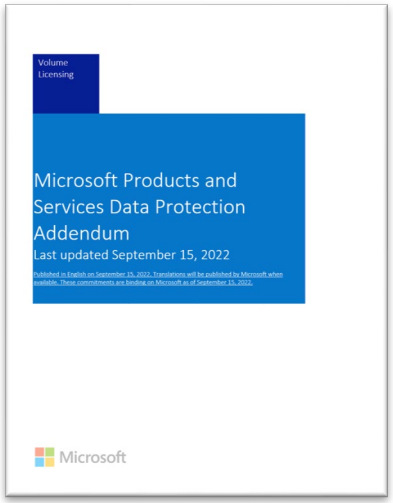
This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	September 15, 2022	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Microsoft Ireland Operations Limited Trading name (if different): Main address (if a company registered address): One Microsoft Place South County Business Park Leopardstown, Dublin 18 D18 P521, Ireland Official registration number (if any) (company number	Full legal name: Microsoft Corporation Trading name (if different): Main address (if a company registered address): Microsoft Corporation Attn: Chief Privacy Officer One Microsoft Way Redmond, WA 98052 USA Official registration number (if any) (company number or similar identifier):

VERSION B1.0, in force 21 March 2022 1



Volume Licensing

Microsoft Products and Services Data Protection Addendum

Last updated September 15, 2022

Published in English on September 15, 2022. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of September 15, 2022.

Microsoft

Lösungsansätze

Standardvertragsklauseln (Standard Contractual Clauses (SCC))

Um die Anforderungen aus «Schrems II» zu adressieren, hat Microsoft ihre Standardvertragsklauseln angepasst. Um die Übertragung von personenbezogenen Daten von Kunden in der EU in Länder ausserhalb des Europäischen Wirtschaftsraums (EWR) zu regeln, hat Microsoft den «Processor-to-Processor» Ansatz gewählt.

Data Protection Addendum (DPA)

- **Keine permanenten Zugriffsrechte**
  Microsoft garantiert vertraglich, dass keine permanenten Zugriffsrechte für Microsoft Mitarbeiter oder Unterauftragsverarbeiter möglich sind. Der Zugriff ist über verschiedene Zugriffskontrollen gesichert und auditiert. Die Einhaltung dieser technischen Kontrollen kann mittels der unabhängigen Audit Reports überprüft werden.
- **Unterauftragsverarbeiter**
  Microsoft ist dafür verantwortlich, dass alle Unterauftragsverarbeiter die Verpflichtungen von Microsoft aus dem DPA einhalten.
  Die Liste der Unterauftragsverarbeiter, deren Serviceverantwortung und deren Firmenstandort sind veröffentlicht.

Herausforderung III: Microsoft Support

Problemstellung

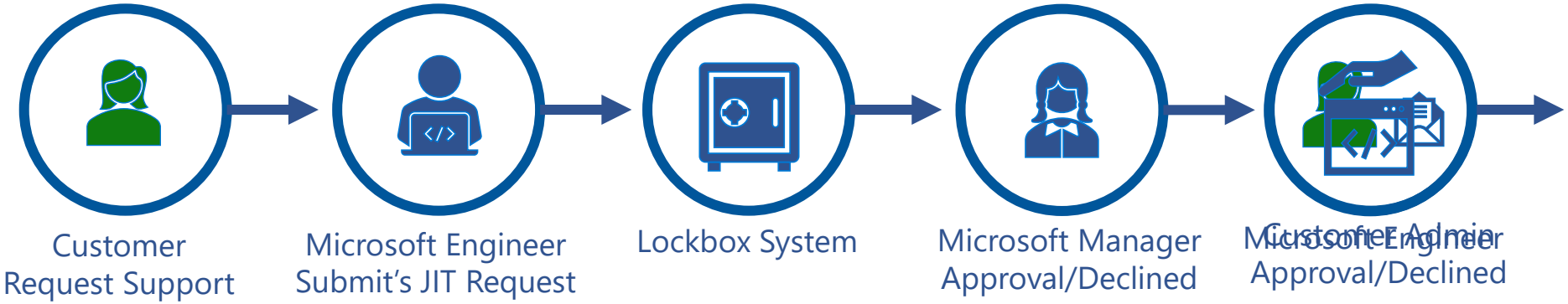
Das heutige Supportmodell von Microsoft basiert auf dem «Follow-the-Sun» Konzept. Damit kann es zu Situationen kommen, bei welchen für die Bearbeitung eines Cases Supportmitarbeiter ausserhalb von Europa zugreifen müssen.

Lösungsansätze

Customer Lockbox

Der Standard Lockbox Prozess muss zwingend für alle Zugriffe angewendet werden. Damit können die Zugriffsrechte protokolliert, kontrolliert und auch eingeschränkt werden.

Der Customer Lockbox Prozess ermöglicht dem Kunden zusätzlich den finalen Entscheid über den Zugriff zu steuern.



Investitionen von Microsoft in die Initiative “EU Data Boundary”

«EU Data Boundary» Initiative

Daten verbleiben in der EU

Gestaltung der Enterprise Services um Kunden-, Support- und Personendaten innerhalb der EU zu speichern und zu verarbeiten.

Support in EU

Support wenn möglich aus EU anbieten und Neugestaltung der Support-Tools, die Microsoft derzeit verwendet, um personenbezogene Daten in der EU zu belassen.

Erweiterung EU-Rechenzentren

Erweiterung der Anzahl der EU-Rechenzentren und Erhöhung der Kapazität in bereits bestehenden, um der verstärkten Verarbeitung und Speicherung in der EU gerecht zu werden.

Sicherer Fernzugriff

Implementierung von Technologien wie Virtual Desktop Infrastructure (VDI), um den Fernzugriff auf personenbezogene Daten zu schützen und dadurch die physische Übertragung von Daten zu verhindern.

Erhöhung der Transparenz rund um die Sicherheit

Während wir weiterhin die Sicherheit gewährleisten – ein wichtiger Teil des Datenschutzes – erhöhen wir die Transparenz darüber, wie und zu welchem Zweck Daten verwendet werden.

Reduzierung der Unterauftragsverarbeiter

Begrenzung der Anzahl der Unterauftragsverarbeiter, die auf personenbezogene Daten von EU-Kunden zugreifen können.

Quelle: EU Data Boundary for the Microsoft Cloud: A progress report

Zusammenfassung

Speicherort der Daten

Aufgrund rechtlicher Anforderungen müssen Daten in bestimmten Regionen gespeichert werden (z.B. CH oder EU) und dürfen nicht ins (unsichere) Ausland transferiert werden.

Zusätzliche Informationen

- Speicherorte für Office 365
- Verfügbarkeit von Azure Services

Zugriffe durch Microsoft

Der Zugriff auf Kundendaten durch Microsoft (oder Unterauftragsverarbeiter) von ausserhalb Europas kann problematisch sein, da das Datenschutzniveau nicht mit dem der Schweiz übereinstimmt.

Zusätzliche Informationen

- Standard Contractual Clauses
- Data Protection Addendum
- Liste Unterauftragsverarbeiter
- Service Trust Portal (z.B. Audit Reports)

Microsoft Support

Das heutige Supportmodell von Microsoft basiert auf dem «Follow-the-Sun» Konzept. Damit kann es zu Situationen kommen, bei welchen für die Bearbeitung eines Cases Supportmitarbeiter ausserhalb von Europa zugreifen müssen.

Zusätzliche Informationen

- Data Protection Addendum
- Customer Lockbox for Office 365

Vielen Dank für Ihre Aufmerksamkeit!