



MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Azure Services im öffentlichen Sektor der Schweiz

Version 1.4

Zugehörige Dokumente

Dokumentname

Microsoft Public Sector Cloud Design

Dokument: Cloud Governance & Security im öffentlichen Sektor der Schweiz V1.4

Identifikation: Governance and Security Guideline Swiss Public Sector_V1.4

Azure Blueprints for Public Sector (ISO 27001)

[Microsoft Docs](#)

© (2021) Microsoft Corporation. All rights reserved. Microsoft, Windows and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational and discussion purposes only and represents the current view of Microsoft Corporation or any Microsoft Group affiliate as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment or binding offer or acceptance of any warranties, liabilities, wrongdoing etc. on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.

Inhalt

| | | |
|-------|--|----|
| 1 | Einleitung zum Microsoft Public Sector Cloud Design – MPSD | 5 |
| 1.1 | Kontrolle von Daten als Kernthema | 5 |
| 2 | Rechtliche Herausforderungen beim Cloud Design | 6 |
| 2.1 | Übersicht | 6 |
| 2.1.1 | Cloud Computing als eigener Auslagerungssachverhalt | 6 |
| 2.1.2 | Ausland | 6 |
| 2.2 | Gesetzliche Regelungen | 7 |
| 2.2.1 | Allgemeines | 7 |
| 2.2.2 | Die gängigsten Vorgaben im Einzelnen | 7 |
| 2.3 | Informationsschutzverordnung (ISchV) | 12 |
| 3 | Kontrollziele und Risiken | 13 |
| 3.1 | Kontrollziele | 13 |
| 3.2 | Risikoanalyse | 14 |
| 4 | Massnahmen und Komponentenbeschrieb | 17 |
| 4.1 | M1 – Azure Blueprint – ISO 27001 | 17 |
| 4.2 | M2 – Azure Purview | 18 |
| 4.3 | M3 – Azure Resources Tags | 19 |
| 4.4 | M4 – Azure Key Vault | 19 |
| 4.5 | M5 – Azure IAM (Role Based Access Control RBAC) | 20 |
| 4.6 | M6 – Azure Policies | 21 |
| 4.7 | M7 – Azure Monitor | 21 |
| 4.8 | M8 – Microsoft Compliance Manager für GDPR / DSGVO | 22 |
| 4.9 | M9 – Azure Data Subject Requests für GDPR / DSGVO | 23 |
| 4.10 | M10 – Schulung für Microsoft Public Sector Cloud Design | 23 |
| 4.11 | M11 – Kunden-Lockbox für Azure | 24 |
| 4.12 | M12 – Azure Stack Hub | 25 |
| 4.13 | M13 – Azure Stack HCI | 25 |
| 4.14 | M14 – Azure Arc | 26 |
| 4.15 | M15 – Vertragswerk | 27 |
| 4.16 | M16 – Shared Responsibility Model | 29 |
| | Appendix: Wichtige Vertragsgrundlagen und Links | 30 |

Tabellen

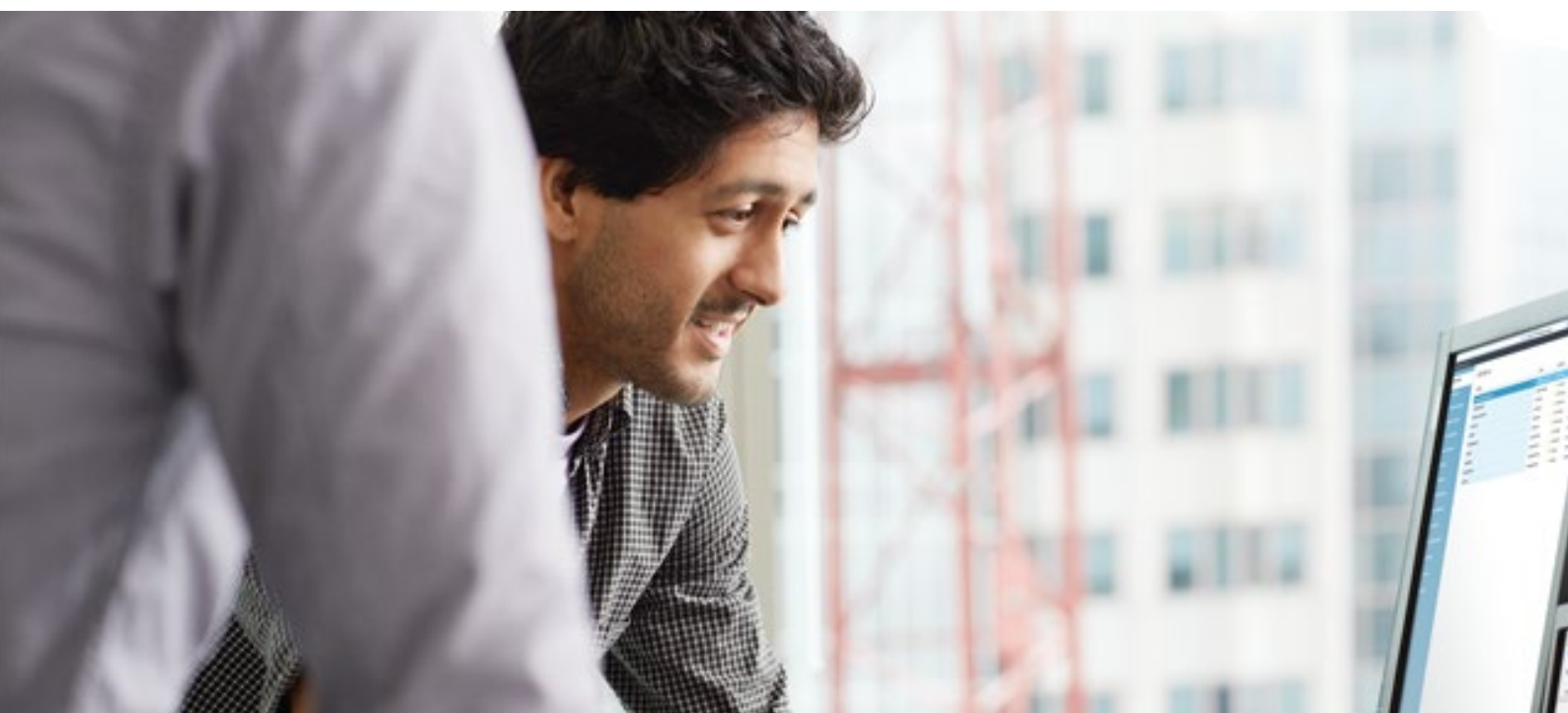
| | |
|---|----|
| Tabelle 1 – Matrix Klassifizierungsstufen und Massnahmen nach ISchV | 12 |
| Tabelle 2 – Kontrollziele der Informationssicherheit | 14 |
| Tabelle 3 – Risikoanalyse aufgrund gesetzlicher Grundlage und Grundlagen der Informationssicherheit | 16 |
| Tabelle 4 – Massnahmenliste | 17 |
| Tabelle 5 – Zusammenstellung wichtiger Informationsquellen | 30 |

Abbildungen

| | |
|---|----|
| Abbildung 1 – ISO 27001 Blueprint 1 | 18 |
| Abbildung 2 – Azure Purview | 19 |
| Abbildung 3 – Azure Key Vault | 20 |
| Abbildung 4 – Azure IAM (RBAC) | 20 |
| Abbildung 5 – Azure Policies | 21 |
| Abbildung 6 – Azure Monitor | 22 |
| Abbildung 7 – Microsoft Compliance Manager für GDPR | 22 |
| Abbildung 8 – Azure Data Subject Requests für GDPR | 23 |
| Abbildung 9 – Schulung in Microsoft Public Sector Cloud Design | 24 |
| Abbildung 10 – Kunden-Lockbox | 24 |
| Abbildung 11 – Azure Stack Hub | 25 |
| Abbildung 12 – Azure HCI | 26 |
| Abbildung 13 – Azure Arc | 27 |
| Abbildung 14 – Microsoft Assurance Framework | 27 |
| Abbildung 15 – Beziehung der Cloud-Governance des Kunden und dem Microsoft Assurance Framework | 28 |
| Abbildung 17 – Shared Responsibility Modell | 29 |

Disclaimer

Dieses Dokument enthält eine allgemeine Darstellung von Fragen, die unsere Kunden beim Einsatz von Cloud Computing Lösungen häufig stellen. Sie sollen damit in die Lage versetzt werden, die technischen und rechtlichen Hintergründe beim Einsatz einer Cloud Computing Lösung besser zu verstehen. Dieses Dokument beinhaltet keine einzelfallbezogene Prüfung individueller Rechtsverhältnisse. Für die individuelle und abschliessende rechtliche Beurteilung über die Zulässigkeit des Einsatzes von Microsoft Cloud Lösungen in einem konkreten Anwendungsfall müssen Sie daher eine separate rechtliche Beratung in Anspruch nehmen.



1 EINLEITUNG ZUM MICROSOFT PUBLIC SECTOR CLOUD DESIGN – MPSD

Die Nutzung von Cloud-Lösungen ist mittlerweile weit verbreitet und erhält mit der wachsenden Zahl von leicht zugänglichen Angeboten auch bei Behörden zunehmend Zuspruch. Den offensichtlichen Vorteilen stehen Herausforderungen gegenüber, welchen die Behörden Rechnung zu tragen haben: Die Daten liegen beim Cloud-Anbieter, bleiben aber unter der Kontrolle der Behörde. Man spricht davon, dass die sog. Datenbearbeitung an den Cloud-Anbieter «ausgelagert» wird. Zur Sicherstellung der Kontrolle über die ausgelagerte Datenbearbeitung muss sich die Behörde mit den Verhältnissen beim Cloud-Anbieter auseinandersetzen, insbesondere mit Blick auf die Informationssicherheit.

Die Fragestellung ist somit, welche Hilfestellung Microsoft als Cloud-Service-Provider seinen Kunden aus dem öffentlichen Sektor bieten kann, wenn sich diese für die Nutzung von Microsoft Online Services entscheiden. Welche daraus resultierenden Risiken müssen die Kunden aus dem Behördenumfeld kennen und welche vertraglichen, organisatorischen und technischen Mittel Microsoft bereitstellt, damit die Online Services sicher genutzt werden können.

1.1 KONTROLLE VON DATEN ALS KERNTHEMA

Cloud-Lösungen zielen darauf ab, dass Daten anstatt auf eigenen lokalen Computern oder Servern auf technischen Infrastrukturen von spezialisierten Drittanbietern wie beispielsweise Microsoft bearbeitet werden. Eine solche Datenbearbeitung durch Dritte ist rechtlich grundsätzlich zulässig unter der Voraussetzung, dass nebst der Einhaltung der fallspezifischen Compliance-Anforderungen insbesondere auch sichergestellt ist, dass der für die Daten Verantwortliche «die Kontrolle behält».

Kontrolle heisst in diesem Zusammenhang einerseits, dass mittels technischer, organisatorischer und vertraglicher Massnahmen gewährleistet ist, dass nur befugte Personen auf die Daten Zugriff haben und die datenschutzrechtlichen Pflichten (Sicherheitsmassnahmen, Meldepflichten, Einhaltung der Bearbeitungsgrundsätze etc.) eingehalten werden. Andererseits muss sichergestellt sein, dass die zugriffsberechtigten Dritten die Daten nicht unbefugt verwerten und sie die Daten auf Aufforderung des für die Daten Verantwortlichen wirklich endgültig löschen. Im Fall von Cloud-Lösungen beinhaltet das Kontrollerfordernis insbesondere auch die Anforderung, dass die entsprechende Auslagerung bei Bedarf mit vernünftigen zeitlichem und sachlichem Aufwand wieder auf die eigene oder auf eine andere Infrastruktur rück- bzw. überführbar ist.

Welche konkreten Anforderungen zu erfüllen sind, hängt von den Umständen sowie der Art der Daten ab. Beispielsweise sind die Anforderungen höher, wenn Daten unverschlüsselt an den Drittanbieter übermittelt werden (wobei die Datenübermittlung zu Azure Services generell immer verschlüsselt ist) oder deren Verwertung durch einen unbefugten Dritten die betroffenen Personen empfindlich treffen könnte (z.B. Amtsgeheimnisdaten).

Das Erfordernis der «Kontrolle» ist nicht ausdrücklich in einem Gesetz oder einer einzelnen übergeordneten Gesetzesbestimmung statuiert. Implizit zielen aber alle informationsrechtlich relevanten Erlasse des Bundesrechts und der kantonalen Gesetzgebung darauf ab, die Kontrollansprüche auf Informationen zu organisieren. Kontrolle als Pflicht ist also gewissermassen das abstrakte «Destillat», das verbleibt, wenn man die relevanten gesetzlichen Einzelnormen gedanklich auf das Wesentliche reduziert.

Auch die Instrumente zur Ausübung und Sicherstellung der Kontrolle von Daten sind bei lokalen IT-Infrastrukturen und Cloud-Lösungen grundsätzlich deckungsgleich, nämlich technische, organisatorische und vertragliche Massnahmen.

2 RECHTLICHE HERAUSFORDERUNGEN BEIM CLOUD DESIGN

2.1 ÜBERSICHT

Obwohl sich der Grundsatz «Cloud first» bereits in einer vor bald zehn Jahren verabschiedeten «Cloud Computing Strategie der Schweizer Behörden» findet, besteht behördenseitig auch heute noch eine gewisse Zurückhaltung, was sich wohl auf bestehende Unsicherheiten im Umgang mit Cloud-Lösungen zurückführen lässt. In der Cloud Strategie 2020 ist acht Jahre nach dem Entscheid für den Grundsatz «Cloud First» immerhin noch (oder schon) von einem **Paradigmenwechsel hin zu «Cloud First»** die Rede (Cloud-Strategie 2020)¹.

Die **Unsicherheiten** sind bei Behörden auf allen föderalen Ebenen, d.h. Bundes-, Kantons- und Gemeindebehörden zu beobachten. Während für Bundesbehörden das Datenschutzgesetz und weitere Erlasse des Bundes im Vordergrund stehen, haben sich kantonale Behörden und Gemeindebehörden an das Datenschutzgesetz und ggf. weitere Erlasse des jeweiligen Kantons zu halten. Was für Behördenmitglieder auf allen Ebenen gilt, ist das Amtsgeheimnis bzw. die Strafbarkeit von Behördenmitgliedern bei Verletzung desselben.

2.1.1 Cloud Computing als eigener Auslagerungssachverhalt

Im Rahmen von Cloud-Lösungen werden Daten anstatt auf eigenen lokalen Computern oder Servern auf entsprechenden IT-Infrastrukturen von Drittanbietern bearbeitet und durch Fremdpersonal verwaltet. Es liegt daher ein sog. Auslagerungssachverhalt im Sinne der Datenschutzgesetzgebungen vor.

Cloud-Lösungen sollten aber von klassischen Outsourcing-Lösungen unterschieden werden, welche ebenfalls als Auslagerungssachverhalt nach den einschlägigen Datenschutzbestimmungen qualifizieren. Als «klassisches» Outsourcing wird typischerweise der Fall verstanden, wonach ein Dienstleister nach Massgabe von spezifischen Weisungen des Kunden an dessen Stelle Geschäftsabläufe steuert und in diesem Zusammenhang Datenzugriff und -einsicht erhält. Demgegenüber bezieht der Kunde in einem Cloud-Modell grundsätzlich eine **standardisierte Leistung**. Die **Individualität bzw. die fehlende Individualität** der Leistungsbeziehung (technische und organisatorische Ebene) ist somit ein zentrales Abgrenzungskriterium zwischen Cloud Computing und klassischem Outsourcing. Der Übergang zwischen beiden Formen ist indes fließend.

2.1.2 Ausland

Werden im Rahmen von Cloud-Lösungen Personendaten in Ländern bearbeitet, die ein tieferes Datenschutzniveau aufweisen als in der Schweiz bzw. in der EU oder dem EWR (man spricht von «fehlender Gleichwertigkeit» im sog. «unsicheren Ausland»), ist die Zulässigkeit der entsprechenden Datenbearbeitung über das allgemeine Erfordernis der Kontrolle hinaus von der Erfüllung zusätzlicher Bedingungen abhängig (z.B. Bestehen vertraglicher Schutzmassnahmen, siehe auch 4.15).

¹ <https://www.news.admin.ch/news/message/attachments/64425.pdf>

2.2 GESETZLICHE REGELUNGEN

2.2.1 Allgemeines

Da der Bund keine umfassende Kompetenz zur Gesetzgebung im Bereich des Datenschutzes hat, sind die Kantone aufgrund ihres Rechts zur eigenen Organisation befugt, den Datenschutz selbständig zu regeln, soweit es um die Bearbeitung von Personendaten durch kantonale Behörden, Gemeinden und Verwaltungsstellen geht. Sämtliche Kantone verfügen über allgemeine Datenschutzerlasse. Diese konkretisieren den grundrechtlichen Persönlichkeitsschutz und die rechtsstaatlichen Grundsätze für das Bearbeiten von Personendaten auf kantonaler Ebene, indem sie die Voraussetzungen und allgemeinen Grundsätze der Datenbearbeitung durch kantonale und kommunale Behörden sowie die Rechte der betroffenen Personen festlegen. Wenn sich kantonale öffentliche Organe am privaten wirtschaftlichen Wettbewerb beteiligen, ist diese Tätigkeit nicht der Ausübung hoheitlicher Funktionen oder der Ausübung öffentlicher Aufgaben des kantonalen Rechts zuzuordnen (so z.B. bei Kantonalbanken).

Im nationalen DSG und den meisten kantonalen Datenschutzgesetzen finden sich besondere Vorschriften für die sog. Auftragsdatenbearbeitung. Eine solche liegt vor, wenn das verantwortliche öffentliche Organ einen Dritten damit betraut, einen Datenbearbeitungsvorgang auszuführen.

In gewissen Kantonen finden sich spezifische Vorschriften zu den Voraussetzungen einer Auslagerung von Datenbearbeitungsvorgängen an Dritte (z.B. die Vereinbarung in einem schriftlichen Vertrag, spezifische Regelungen zum Beizug von Unterauftragsbearbeitern etc.). Die meisten Kantone stellen diesbezüglich jedoch keine besonderen, über die Regelungen im DSG hinausgehende, Regeln auf.

Im Allgemeinen kann gesagt werden, dass die Auftragsdatenbearbeitung grundsätzlich zulässig ist, wenn keine gesetzlichen oder vertraglichen Geheimhaltungspflichten entgegenstehen und die Einhaltung der datenschutzrechtlichen Vorschriften gewährleistet ist. Insofern ist das Grundprinzip im Datenschutzgesetz des Bundes und den kantonalen Datenschutzgesetzen vergleichbar.

Grundsätzlich bleibt das öffentliche Organ, das den Auftrag erteilt, für die Einhaltung des Datenschutzes verantwortlich. Es hat geeignete Massnahmen zu ergreifen, um ein angemessenes Datenschutzniveau sicherzustellen.

2.2.2 Die gängigsten Vorgaben im Einzelnen

2.2.2.1 Vertragliche Vereinbarung

Mit Dritten, welche ausgelagerte Datenbearbeitungen für eine Behörde übernehmen (z.B. Microsoft), ist ein Auslagerungsvertrag abzuschliessen, der Absicherungen mit Blick auf die Einhaltung von Datenschutz und Datensicherheit sowie den Einsatz der Cloud-Dienste im öffentlich-rechtlichen Bereich regelt.

Je nach Kanton bestehen gesetzliche Regelungen, welche Vorgaben bezüglich des Inhalts des Vertrages mit dem Auftragsbearbeiter machen. In einigen Kantonen bestehen auch sog. Allgemeine Geschäftsbedingungen, welche als Bestandteil von Verträgen zur Auslagerung von Informatikleistungen bzw. der Bearbeitung von Personendaten zu vereinbaren sind.² Von diesen Vorgaben kann im Interesse einer geeigneten Lösung grundsätzlich abgewichen werden, namentlich insofern, als sich aus der Rechtslage keine zwingenden Gründe ergeben, solche AGB unverändert zur Anwendung zu bringen resp. wo eine Prüfung ergibt, dass den Anforderungen an genügende vertragliche Regelungen bezüglich Datenschutz und Datensicherheit auch auf Basis der Vertragswerke des Anbieters genügend Rechnung getragen wird.

Entsprechend der Natur einer «Cloud» mit standardisierten Angeboten für alle Kunden setzt Microsoft Standardverträge für die Nutzung der Cloud-Infrastruktur ein. Die Berücksichtigung individueller Anforderungen in grösserem Umfang ist auf der gegebenen hochstandardisierten IT-Infrastruktur schwierig und muss im Einzelfall geklärt werden, wozu Microsoft grundsätzlich Hand bietet.

² Z.B. Kanton Bern (Allgemeine Geschäftsbedingungen über die Informationssicherheit und den Datenschutz bei der Erbringung von Informatikdienstleistungen); Kanton Zürich (Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen)

2.2.2.2 Bearbeitung nach Weisung und im Interesse des öffentlichen Organs

Der Auftragsbearbeiter darf die Datenbearbeitungen nur nach Weisung und im Interesse des öffentlichen Organs vornehmen. Art. 10a Abs. 1 lit. a DSGVO sowie verschiedene kantonale Gesetzgebungen enthalten diesbezüglich Bestimmungen, dass die Daten nur so bearbeitet werden dürfen, wie es das öffentliche Organ selbst tun dürfte.

Die Datenschutzbestimmungen von Microsoft (Data Protection Addendum, DPA)³ halten dies fest. Microsoft als Auftragsdatenbearbeiterin wird Kundendaten (und insbesondere Personendaten) nur in Übereinstimmung mit den dokumentierten Anweisungen des Kunden und wie in den Datenschutzbestimmungen beschrieben bearbeiten, um (a) dem Kunden die Onlinedienste zur Verfügung zu stellen und (b) für die mit der Bereitstellung der Onlinedienste an den Kunden verbundenen rechtmässigen Geschäftsvorgänge von Microsoft. Das jeweilige Vertragswerk des Kunden zusammen mit der Produktdokumentation und der Verwendung und Konfiguration der Funktionalitäten der Onlinedienste stellen diesbezüglich zusammen die vollständigen und endgültigen Weisungen des Kunden an Microsoft für die Bearbeitung von Kundendaten dar.

Kundendaten werden insbesondere nicht für Zwecke der Werbung, Marktforschung oder der Benutzerprofilerstellung verwendet.

2.2.2.3 Einbezug weiterer Datenbearbeiter

Das DPA beschreibt im Abschnitt «Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern», wie Microsoft mit Unterauftragnehmern umgeht und Kunden über Änderungen im Portfolio der Unterauftragnehmer etc. benachrichtigt. Darin wird beschrieben, welche Anforderungen Microsoft an Unterauftragsverarbeiter stellt, und dass Microsoft dafür verantwortlich ist, dass die Unterauftragnehmer alle Anforderungen erfüllen, die Teil des DPA sind.

Das Services Trust Center⁴ führt die Liste, einschliesslich der von ihnen erbrachten Dienste, des Standorts ihres Hauptsitzes und des Umfangs und der Bedingungen, unter denen sie auf Kundendaten zugreifen können: <http://aka.ms/mscloudsubprocessors>.

In den Core Online Services haben weder Microsoft noch Unterauftragnehmer ständigen administrativen Zugriff auf Kundendaten oder Kundenlösungen. Microsoft Cloud arbeitet mit «Zero standing ADMIN» auch bekannt als «Least Privilege», bei dem der administrative Zugriff durch ein Authentifizierungsverfahren (genannt «Lockbox») kontrolliert wird, z.B. im Fall von Kunden, die Microsoft mit einer Supportaufgabe beauftragen, die dem mit dem Supportfall betrauten Mitarbeiter Privilegien einräumen (welche einen zeitlich begrenzten Zugriff auf Kundendaten ermöglichen könnten). Die Zuteilung des administrativen Zugriffs muss über mehrere Verknüpfungen, Time-Boxen und ein vollständiges Audit-Protokoll erfolgen – und kann, wenn der Kunde es wünscht, auch die endgültige Genehmigung durch den Kunden beinhalten, indem ein erweiterter «Lockbox»-Prozess eingerichtet wird, genannt «Customer Lockbox» (siehe Kapitel 4.11).

2.2.2.4 Datensicherheit

Die nationalen und kantonalen Datenschutz- und Informationssicherheits-Gesetzgebungen verlangen im Zusammenhang mit der Auslagerung von Informatikleistungen resp. der Auftragsdatenbearbeitung in der Regel die Gewährleistung einer angemessenen Datensicherheit durch den Auftragnehmer. Dabei definieren die meisten kantonalen Erlasse keine konkreten Schutzmassnahmen, sondern legen Grundsätze bezüglich der abzusichernden Schutzziele – **Vertraulichkeit, Verfügbarkeit und Integrität** – fest. Insbesondere müssen dabei die folgenden Risiken abgesichert werden:

- Unbefugte oder zufällige Vernichtung
- Zufälliger Verlust
- Technischer Fehler
- Fälschung, Diebstahl oder widerrechtliche Verwendung
- Unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen

Personendaten müssen durch **angemessene technische und organisatorische Massnahmen** gegen solche Risiken geschützt werden.

Microsoft verwendet in den Onlinediensten zahlreiche Verschlüsselungen auf verschiedensten Ebenen und hat hierzu umfassende Dokumentationen und Whitepapers veröffentlicht. Einerseits werden verschiedene Verschlüsselungen für gespeicherte Daten («data at rest») angewandt, und zwar sowohl auf den Betriebsumgebungen («Volume Level») als auch auf den einzelnen Datenfiles, somit ist ein physikalischer Zugriff auf die Daten ausgeschlossen. Der Verschlüsselungsschutz kann durch die Nutzung von selbst verwalteten Schlüsseln, sog. BYOK («Bring Your Own Key») noch ergänzt werden. Microsoft wendet zudem auch bei der Datenübertragung («data in-transit») Verschlüsselungstechniken an. Darüber hinaus bieten die

³ Microsoft-Onlinedienste – Nachtrag zum Datenschutz: <https://aka.ms/dpa>

⁴ <https://servicetrust.microsoft.com>

Onlinedienste verschiedene weitere Wege für den Cloud-Kunden selbst an, gewisse eigene Verschlüsselungstechniken anzuwenden und zu verwalten.

Über das Microsoft Trust Center⁵ sowie über die Dienstüberprüfung im Security & Compliance Center⁶ können Cloud-Kunden Zertifizierungs- und Audit-Prüfberichte sowie weitere umfassende Informationen über die Datenhaltungsstandorte, Zugriffsmöglichkeiten auf Daten des Cloud-Kunden, Sicherheitsvorkehrungen und Datenschutzvorkehrungen jederzeit direkt einsehen. Auf diesem Weg kann sich der Cloud-Kunde jederzeit von der Einhaltung der Sicherheitspflichten durch Microsoft überzeugen.

2.2.2.5 Auslandsbezüge

Die Datenschutzgesetze des Bundes und der Kantone stellen besondere Anforderungen auf, wenn Personendaten im Rahmen der Verarbeitung in Cloud-Umgebungen ins Ausland transferiert werden oder aus dem Ausland darauf zugegriffen wird.

Im Allgemeinen gilt, dass Auslagerungen in ein Land, welches über ein mit der Schweiz gleichwertiges Datenschutzniveau verfügt, ohne weitere Massnahmen zulässig sind. Dazu gehören insbesondere sämtliche EU/EWR Staaten.

Microsoft nutzt für SaaS Onlinedienste für schweizerische Cloud-Kunden standardmässig die Rechenzentren der Region Schweiz und teilweise der Region Europa (mit Rechenzentren in Irland, Niederlanden, Österreich und Finnland). Die Kundendaten werden in diesen Rechenzentren gespeichert. Die jeweiligen Datenhaltungsstandorte können für jeden Onlinedienst über die jeweilige Dienstüberprüfung im Security & Compliance Center⁷ abgerufen werden.

Die konkrete Bereitstellung der Onlinedienste oder dessen individuelle Konfiguration durch den Kunden kann es im Einzelfall notwendig machen, dass einige Kundendaten an Mitarbeiter oder Subunternehmer von Microsoft ausserhalb dieser primären Speicherregion zugänglich gemacht werden. Ebenfalls kann es vorkommen, dass sich diejenigen Microsoft Mitarbeiter mit der meisten technischen Erfahrung für die Behandlung spezieller Dienstprobleme an Standorten ausserhalb dieser primären Speicherregion befinden, und diese dann gegebenenfalls online Zugriff auf Systeme oder Daten benötigen, um ein Problem lösen zu können.

Gemäss den Microsoft Datenschutzbestimmungen für Onlinedienste darf deshalb Microsoft Kundendaten, die Microsoft im Namen des Cloud-Kunden bearbeitet, grundsätzlich auch in andere Länder, in denen Microsoft oder ihre verbundenen Unternehmen oder Subunternehmer Einrichtungen haben (mitunter auch in die USA), übertragen, dort speichern und bearbeiten. Microsoft verpflichtet sich dabei, jederzeit die Anforderungen der Datenschutzgesetze der Schweiz in Bezug auf die Erfassung, Nutzung, Übertragung, Aufbewahrung und sonstige Bearbeitung personenbezogener Daten aus der Schweiz einzuhalten.

⁵ <https://www.microsoft.com/de-ch/trust-center>

⁶ <https://docs.microsoft.com/de-ch/microsoft-365/compliance/service-assurance?view=o365-worldwide>

⁷ <https://docs.microsoft.com/de-ch/microsoft-365/compliance/service-assurance?view=o365-worldwide>



Für potenzielle Transfers von Kundendaten, Professional Services Daten und Personendaten aus der EU/EWR und der Schweiz in sog. unsichere Drittländer hat Microsoft sog. Standardvertragsklauseln (Processor-to-Processor) zwischen Microsoft Ireland Operations Ltd. und Microsoft Corp. USA abgeschlossen. Die Standardvertragsklauseln wurden für Datenexporte aus der Schweiz gemäss den Empfehlungen des EDÖB auf die schweizerischen Verhältnisse angepasst.

Microsoft hat am 6. Mai 2021 angekündigt, mit der sog. EU Data Boundary die Core Online Services Azure, Microsoft 365, Dynamics 365 und Power Platform technisch so auszugestalten, dass die Kernkundendaten innerhalb Europa bearbeitet und gespeichert werden sowie der Support aus dem Europäischen Raum erbracht wird.⁸ Erklärtes Abschlussziel ist Ende 2022.

Microsoft wird zudem Kundendaten nicht an Strafverfolgungsbehörden weitergeben, es sei denn, dies ist gesetzlich vorgeschrieben. Wenn sich Strafverfolgungsbehörden an Microsoft wenden, um Daten des Kunden anzufordern, wird Microsoft versuchen, die Strafverfolgungsbehörde umzuleiten, damit sie diese Daten direkt vom Kunden anfordert. Wenn Microsoft gezwungen ist, Strafverfolgungsbehörden Daten offenzulegen oder Zugang zu ihnen zu gewähren, wird Microsoft den Kunden unverzüglich benachrichtigen und eine Kopie der Anforderung bereitstellen, sofern dies nicht gesetzlich verboten ist. Microsoft verfolgt einen prinzipiellen und strengen Ansatz im Umgang mit behördlichen Anfragen nach Zugriff auf Kundendaten, die sich im Gewahrsam von Microsoft befinden.⁹

Microsoft veröffentlicht alle sechs Monate einen sog. «Law Enforcement Request Reports» um Transparenz über den Umfang und die Art dieser Vorfälle zu gewährleisten.¹⁰ Die Berichte sind öffentlich und können zur Unterstützung bei der Durchführung von Risikobewertungen herangezogen werden. Microsoft interagiert tagtäglich mit Kunden und Regierungen auf der ganzen Welt und gestaltet so den internationalen Rechtsrahmen für diese kritischen Themen aktiv mit. Als Leitfaden für diese Arbeit hat Microsoft sechs Prinzipien veröffentlicht, die auch auf den laufenden Bemühungen zum Schutz der Daten von Microsoft-Kunden und zur Verbesserung des Datenschutzes beruhen.¹¹ Microsoft ist der Ansicht, dass die formulierten Prinzipien universelle Rechte und grundlegende Mindestanforderungen darstellen, die den Zugang der Strafverfolgungsbehörden zu Daten in unserer modernen Zeit regeln sollten. Die Anwendung dieser Prinzipien kann von Land zu Land variieren, aber die zugrundeliegenden Prinzipien von Kontrolle und Ausgewogenheit, Rechenschaftspflicht und Transparenz sollten bestehen bleiben.

2.2.2.6 Behördenzugriffe

Microsoft ist der Überzeugung, dass Kunden das Recht haben, durch ihre eigenen Gesetze geschützt zu werden. Microsoft verfolgt einen prinzipienfesten und strengen Ansatz im Umgang mit staatlichen Anfragen nach Zugriff auf Kundendaten, die sich im Gewahrsam von Microsoft befinden.¹² Die wichtigsten Richtlinien, an die sich Microsoft bei all ihren Diensten hält, sind:

- Microsoft gewährt keiner Regierung direkten und ungehinderten Zugang zu den Daten ihrer Kunden, und gibt keiner Regierung die Verschlüsselungsschlüssel oder die Möglichkeit, die Verschlüsselung zu überwinden.
- Wenn eine Regierung Kundendaten haben möchte, muss sie die geltenden rechtlichen Verfahren einhalten. Sie muss uns einen Durchsuchungsbefehl oder einen Gerichtsbeschluss für Inhaltsdaten oder eine prozessuale Anordnung für Subscription-Informationen oder andere Nicht-Inhaltsdaten vorzeigen.
- Alle Anfragen müssen sich auf bestimmte Konten und Identifikatoren beziehen.
- Das Legal Compliance-Team von Microsoft prüft alle Anfragen, um sicherzustellen, dass sie gültig sind, lehnt diejenigen ab, die nicht gültig sind, und stellt nur die angegebenen Daten bereit.
- Zudem gab Microsoft nach dem Schrems-II-Urteil ein Bekenntnis ab, behördliche Anfragen Dritter nach Kundendaten juristisch anzufechten¹³.

Ein Teil von Microsofts Arbeit in Bezug auf Regierungsanfragen beinhaltet die Veröffentlichung von «Law Enforcement Request Reports» alle sechs Monate¹⁴, um Transparenz über den Umfang und die Art dieser Vorfälle zu gewährleisten.

Für eine Bewertung des Risikos von Behördenzugriffen kann es relevant sein, die tatsächlichen Zahlen zum Umfang aus den Microsoft Law Enforcement Request Reports zu berücksichtigen, die unter dem obigen Link verfügbar sind. In weit über 90% der Behördenanfragen geht es um Daten von Microsoft Konsumentenkunden wie z.B. Hotmail oder Skype.

⁸ <https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/>

⁹ Der Prozess ist hier im Detail beschrieben: <https://aka.ms/mslerh>

¹⁰ Hier zu finden: <https://aka.ms/mslerr>

¹¹ «Six Principles for International Agreements Governing Law Enforcement Access to Data»: <https://aka.ms/MS6dataaccessPrinciples>

¹² Der Prozess ist hier im Detail beschrieben: <https://aka.ms/mslerh>

¹³ Siehe auch: <https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/>

¹⁴ <https://aka.ms/mslerr>

Aus diesen Zahlen wird deutlich, dass ...

- ... die Wahrscheinlichkeit, dass ein bestimmter Unternehmenskunde das Ziel einer solchen Anfrage ist, minimal ist,
- ... die Wahrscheinlichkeit, dass eine solche Anfrage NICHT abgelehnt oder umgeleitet wird, noch geringer ist und
- ... die Wahrscheinlichkeit, dass eine solche Anfrage nach Daten, die ausserhalb des Herkunftslandes der Anfrage gespeichert sind, NICHT abgelehnt oder umgeleitet wird, noch viel geringer ist

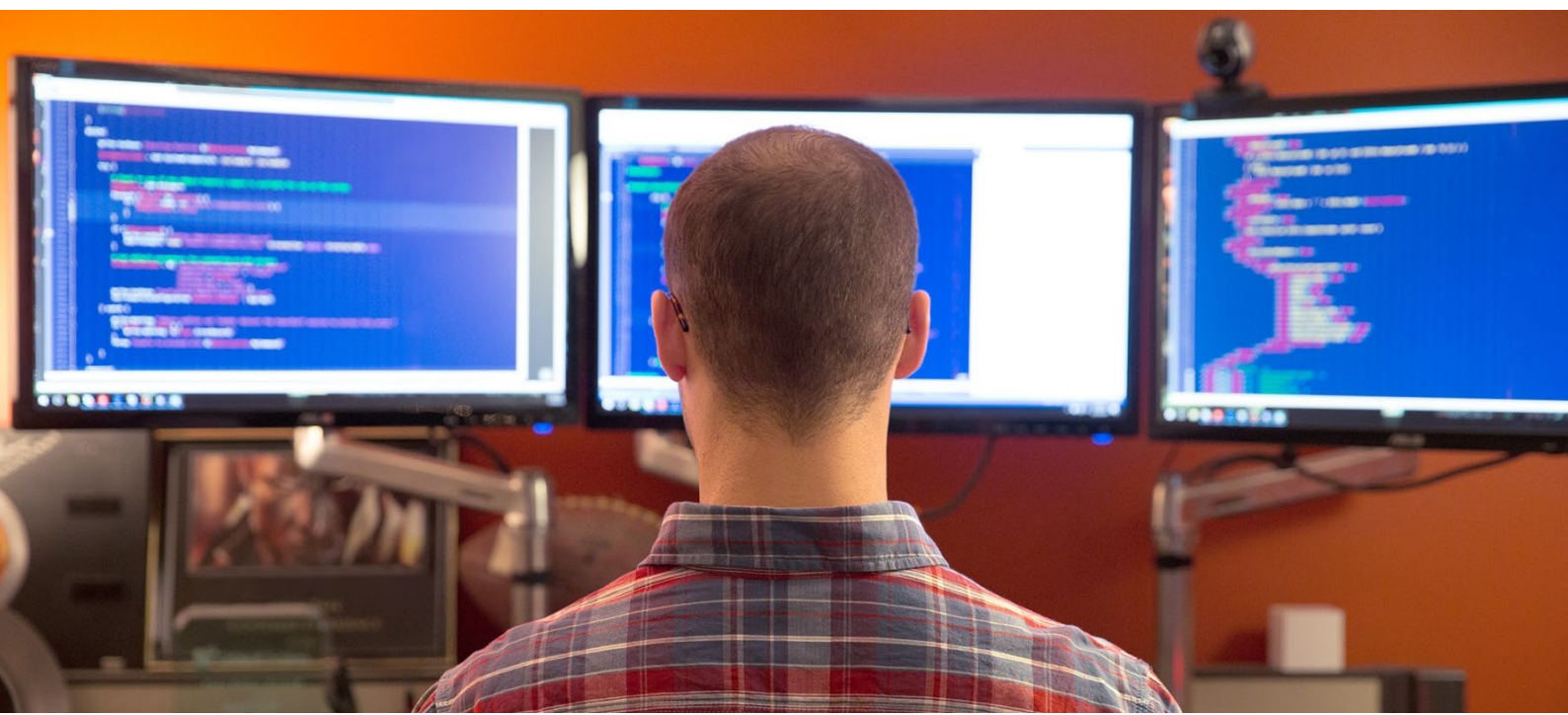
Basierend auf diesen Berichten, einem Verständnis des prinzipiellen Prozesses und der Geschichte von Microsoft zum Schutz der Rechte der Kunden auf Privatsphäre, sollte es für Kunden möglich sein, eine Risikobewertung durchzuführen, die zeigt, dass die Wahrscheinlichkeit und damit das Gesamtrisiko durch Anfragen von Strafverfolgungsbehörden aus Drittländern absolut minimal bis praktisch nicht vorhanden ist.

Zu beachten ist weiter, dass der zahlenmässige Unterschied zwischen Anfragen für Verbraucherkonten und Unternehmenskonten auch die formalen Richtlinien¹⁵ der Abteilung für Computerkriminalität und geistiges Eigentum des US-Justizministeriums widerspiegelt, die Staatsanwälten rät, sich direkt an Unternehmen zu wenden, wenn sie Zugang zu ihren Daten wünschen, wenn dies praktikabel ist und die Ermittlungen nicht anderweitig gefährdet werden, anstatt zu versuchen, über Cloud-Service-Provider zu gehen.

2.2.2.7 Kritische Daten

In Bezug auf ganz bestimmte Informationen, die aufgrund des öffentlichen Interesses, beispielsweise wegen eines besonderen Sicherheitsbezugs zu kritischen Infrastrukturen des Gemeinwesens, nicht in fremde Hände geraten sollten, könnte sich eine ausdrückliche oder implizite Beschränkung zum Einsatz eines Cloud-Dienstes ergeben. Das Gemeinwesen wäre diesbezüglich in der Pflicht, mittels geeigneten Informationsklassifizierungen jene Daten abzugrenzen, die nicht in ein Cloud-Projekt einzubeziehen sind. Solche Aspekte sind im Einzelfall besonders zu planen, und es sind dafür angemessene Massnahmen zu treffen. Das nachfolgende Kapitel behandelt die entsprechenden Grundlagen im Detail.

¹⁵ <https://aka.ms/USDoJSeekingEnterpriseData>



2.3 INFORMATIONSSCHUTZVERORDNUNG (ISCHV)

Die *Verordnung Über Den Schutz Von Informationen Des Bundes* (Informationsschutzverordnung, ISchV, 2015)¹⁶ regelt den Schutz von Informationen des Bundes und der Armee, soweit er im Interesse des Landes geboten ist. Sie legt insbesondere deren Klassifizierung und Bearbeitung fest. Im Kern der Verordnung steht die Zuweisung von Klassifizierungsstufen, welche Informationen entsprechend dem Grad ihrer Schutzwürdigkeit einstuft, und letztlich Massnahmen vorgeschlagen werden oder mindestens davon abgeleitet werden können. Die Verordnung kennt die folgenden 3 Klassifizierungsstufen: GEHEIM, VERTRAULICH, INTERN.

Die folgende Tabelle fasst alle elektronisch anwendbaren Massnahmen der Informationsbearbeitung pro Klassifizierungsstufe zusammen.

| Klasse/ Bearbeitungsvorschrift | INTERN (RESTRICTED ¹⁷) | VERTRAULICH | GEHEIM |
|-----------------------------------|---|--|--|
| Klassifizierungsvermerk (Label) | Vermerk INTERN | Vermerk VERTRAULICH | Vermerk GEHEIM |
| Speicherung bzw. Aufbewahrung | Zugangsgeschützt | Verschlüsselt auf Arbeitssystemen oder entfernbaren Datenträgern | Nur auf bewilligten Mitteln oder verschlüsselt auf Arbeitssystemen oder entfernbaren Datenträgern |
| Datenübertragung | Geschützter Übertragungsweg (z.B. Bundesnetz) | Verschlüsselung oder geschützter Übertragungsweg | Verschlüsselung oder geschützter Übertragungsweg |
| Bearbeitung mit Informatikmitteln | Zulässig | Nur mit von der Koordinationsstelle bewilligten Mitteln (Ausnahme: Armee) und unter Verwendung von Sicherheitssoftware gemäss Bundesstandard | Nur mit von der Koordinationsstelle bewilligten Mitteln und unter Verwendung von Sicherheitssoftware gemäss Bundesstandard |
| Mitnahme ab dauerndem Standort | Zulässig | Eingeschränkt zulässig | Eingeschränkt zulässig |
| Rückzug und Rückgabepflicht | Keine | Zwingend | Zwingend |
| Vernichtung bzw. Löschung | Eingeschränkt zulässig | Eingeschränkt zulässig | Nur durch Verfasser |

Tabelle 1 – Matrix Klassifizierungsstufen und Massnahmen nach ISchV

Die Verordnung gilt überdies auch für Organisationen und Personen des öffentlichen oder privaten Rechts, als auch eidgenössische und kantonale Gerichte, die klassifizierte Informationen bearbeiten, soweit dies im Bundesrecht vorgesehen ist oder entsprechend vereinbart wurde.

¹⁶ <https://www.fedlex.admin.ch/eli/cc/2007/414/de>

¹⁷ Als «RESTRICTED» oder gleichwertig klassifizierte Informationen aus dem Ausland werden wie als INTERN klassifizierte Informationen bearbeitet

3 KONTROLLZIELE UND RISIKEN

Wie auch in anderen Bereichen gibt es auch bei der Cloud-Nutzung kein Gesetz und keine Regelung, welches diese entweder komplett verbietet oder per se erlaubt. Datenschutz-Verantwortliche von öffentlichen Organen müssen daher aufgrund der geltenden Gesetzeslage, der Art der Daten, deren Bearbeitungsform und möglichen Schutz- und Kontrollmassnahmen eine Risikoanalyse durchführen und entscheiden, ob der Schritt in die Cloud vertretbar ist oder nicht.

Das Bewusstsein und die Dokumentation bezüglich der Klassifizierung von Daten und Informationen (vgl. Kapitel 2.3) ist für die Wahl der passenden Massnahmen von zentraler Bedeutung. Sie bildet auch die Grundlage für die Konfiguration und die Überwachung der hinter den Massnahmen stehenden Technologien und Mittel. Basierend auf den Bestimmungen der Informationsschutzverordnung (vgl. Kapitel 2.3) sollte jede Organisation spezifische Massnahmen zum Schutz der jeweiligen Datenklassen vorsehen. Dazu gehören vertragliche, organisatorische, als auch technische Massnahmen. Beispielsweise könnte ein Unternehmen folgende Schutzmassnahmen festlegen:

– Geheime Daten

Geheime Daten werden in einem ersten Schritt nicht in der Cloud abgelegt, sondern lokal gespeichert. Um dabei soweit als möglich von den Sicherheitsfunktionen von Azure zu profitieren, werden die Daten auf einem Azure Stack HCI gespeichert, welcher mittels Azure Arc verwaltet ist.

– Vertrauliche Daten

Vertrauliche Daten dürfen in der Cloud verschlüsselt gespeichert werden. Dazu eignet sich Azure Information Protection (AIP) wahlweise mit einem eigenen Schlüssel (BYOK) oder unter Verwendung von zwei Schlüsseln - einer in Azure und einer lokal beim Kunden (Double Key Encryption).

Es wird in den folgenden Kapiteln darauf verzichtet, Massnahmen auf spezifische Klassifizierungsstufen zuzuweisen. Das Ziel ist vielmehr, die möglichen Kontrollziele und zu behandelnden Risiken vorzuschlagen, welche im Rahmen eines Entscheids für eine Public Cloud berücksichtigt und behandelt werden sollten. Die zu treffenden Massnahmen können im Anschluss abhängig von der Art, Struktur und Information der Daten bestimmt werden.

3.1 KONTROLLZIELE

Als Fundament und Klassifizierungsgrundlage für Risiken und Massnahmen kann das weit verbreitete Modell der Information Security Triad (Informationssicherheits-Triade) beigezogen werden. Es fokussiert dabei auf die drei Hauptbereiche der Informationssicherheit Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit). Es gilt dabei im Wesentlichen, die folgenden, übergeordneten Kontrollziele zu erreichen, bzw. die entsprechenden Fragestellungen beantworten zu können.

| ID | Bereich | Ziel und Beschreibung | Grundlagen |
|-----|---------|--|--|
| KZ1 | C | Zugangskontrolle Sind die Daten im Verantwortungsbereich des Auftragsbearbeiters ausreichend gegen unberechtigten physischen Zugriff geschützt (z.B. Schutz der Vertraulichkeit) | Informationssicherheits-Best Practice (z.B. IKT-Minimalstandard des BWL) Art. 7 und Art. 10a Abs. 2 DSG, Art. 8 und Art. 9 Abs. 1 lit. a VDSG Art. 8 Abs. 1-2 und Art. 9 Abs. 2 revDSG |
| KZ2 | C | Zugriffskontrolle Ist die elektronische Zugriffsberechtigung ausreichend geregelt? | Informationssicherheits-Best Practice (z.B. IKT-Minimalstandard des BWL) Art. 7 und Art. 10a Abs. 2 DSG, Art. 8 und Art. 9 Abs. 1 lit. g VDSG Art. 8 Abs. 1-2 und Art. 9 Abs. 2 revDSG |

| | | | |
|-----|---|--|--|
| KZ3 | C | Verwendungskontrolle Werden Personen mit stehendem oder temporärem Datenzugriff ausreichend kontrolliert, so dass das Risiko der unbefugten Datennutzung minimiert und Verletzungen nachvollzogen werden können? | Informationssicherheits-Best Practice (z.B. IKT-Minimalstandard des BWL) Art. 7 und Art. 10a Abs. 2 DSGVO, Art. 8 und Art. 9 Abs. 1 lit. d und h VDSG Art. 8 Abs. 1-2 und Art. 9 Abs. 2 revDSG |
| KZ4 | C | Löschungskontrolle Ist sichergestellt, dass der Unterauftragsbearbeiter die Daten löscht, wenn die Auslagerung endet? | Art. 10a Abs. 1 lit. a DSGVO Art. 9 Abs. 1 lit. a revDSG |
| KZ5 | I | Integritätskontrolle Welche Vorkehrungen sind vorgesehen, um zu verhindern, dass der Auftragsbearbeiter oder eine andere Drittpartei die Daten manipuliert? | Informationssicherheits-Best Practice Art. 7 und Art. 10a Abs. 2 DSGVO Art. 8 Abs. 1-2 und Art. 9 Abs. 2 revDSG |
| KZ6 | A | Verfügbarkeitskontrolle Wie wird die Verfügbarkeit der Daten sichergestellt? | Informationssicherheits-Best Practice (z.B. IKT-Minimalstandard des BWL) Art. 7 und Art. 10a Abs. 2 DSGVO Art. 8 Abs. 1-2 und Art. 9 Abs. 2 revDSG |
| KZ7 | A | Wiederherstellbarkeit Wie wird die Wiederherstellbarkeit der Daten bei Verlust oder Fehlern sichergestellt? | Informationssicherheits-Best Practice Art. 10a Abs. 1 lit. a DSGVO Art. 9 Abs. 1 lit. a revDSG |

Tabelle 2 – Kontrollziele der Informationssicherheit

3.2 RISIKOANALYSE

Die folgende Risikoauflistung mit den im nachfolgenden Kapitel abgeleiteten vertraglichen, organisatorischen und technischen Massnahmen kann von Entscheidungsträgern in öffentlichen Organen bewertet und als Entscheidungsgrundlage verwendet werden. Die Auflistung der Risiken kann bei Bedarf im Falle von zusätzlichen Regelungen (z.B. Kanton oder Gemeinde) erweitert werden. Die Risiken sind von den Kontrollzielen gemäss Kapitel 3.1 abgeleitet und ebenfalls nach der generellen Methode **C-I-A** klassifiziert. Einige der Risiken haben lediglich einen Verweis auf die gesetzliche oder regulatorische Grundlage (**Ges**), da sie sich nur indirekt einem der Hauptbereiche der Informationssicherheit zuordnen lassen. Die Risiken sind bewusst fokussiert auf das Verhältnis des Kunden mit dem Auftragsbearbeiter. Trotzdem hat der Kunde in den meisten Risikobereichen die Möglichkeit, zusätzlich zu den vertraglichen und organisatorischen Massnahmen rund um die Beziehung mit dem Auftragsbearbeiter selbst noch zusätzliche, technische Schutz- und Sicherheitsmassnahmen zu ergreifen, um das entsprechende Risiko zu adressieren. Dies gilt sowohl gegenüber dem Auftragsbearbeiter sowie potenziell unbefugten Drittparteien. Die Frage, welche pro Risiko zusätzlich gestellt werden muss, lautet wie folgt: «Wie und mit welchen Massnahmen kann und soll ich als Kunde komplementär zu den Massnahmen des Auftragsbearbeiters dieses Risiko zusätzlich adressieren?».

Ein Vorschlag für ein Mapping der entsprechenden Massnahmen ist ebenfalls in der nachfolgenden Risikotabelle ausgewiesen. Es handelt sich dabei um Massnahmen des Auftragsbearbeiters (Vertragswerk, Dokumentation) sowie um Massnahmen, welche der Kunde treffen kann.

| ID | Bereich (C-I-A), Gesetz | Risiko | Massnahmen-ID | Risikoausschlagwirkung nach Massnahme | Eintrittswahrscheinlichkeit nach Massnahme | Risikobewertung | Restrisiko mitigiert? |
|----|-------------------------|--|---|---------------------------------------|--|-----------------|-----------------------|
| R1 | Ges | Unterauftragsbearbeiter Ist sichergestellt, dass der Auftragsbearbeiter den Kunden über den Einsatz von Unterauftragsbearbeitern informiert und bei Ersatz oder vor Beizug neuer Unterauftragsbearbeitern dem Kunden ein Widerspruchsrecht gewährt (Art. 9 Abs. 3 revDSG)? Unterstehen die Unterauftragsbearbeiter denselben gesetzlichen und regulatorischen Grundlagen wie der Auftragsbearbeiter? | M15 | | | | |
| R2 | Ges | Ungenügende Datensicherheit Ist sichergestellt, dass der Auftragsbearbeiter die Vertraulichkeit, Integrität und Verfügbarkeit der Personendaten des Kunden angemessen schützt (Art. 10a Abs. 2 DSG Art. 9 Abs. 2 revDSG)? Ist die Auditierung der Einhaltung der entsprechenden Sicherheitsverfahren und Sicherheitsrichtlinien sichergestellt und nachvollziehbar dokumentiert? | M8 M10 M15 M16 | | | | |
| R3 | Ges | Nicht gemeldete Datensicherheitsverletzung Ist sichergestellt, dass der Auftragsbearbeiter Datensicherheitsverletzungen dem Kunden meldet (Art. 10a Abs. 2 DSG Art. 9 Abs. 2 und Art. 24 Abs. 3 revDSG)? Werden vom Auftragsbearbeiter die Dienste hinsichtlich Sicherheitsverletzungen überwacht und proaktiv Optimierungen durchgeführt? | M7 M15 | | | | |
| R4 | Ges | Eigene Zwecke des Auftragsbearbeiters Ist sichergestellt, dass der Auftragsbearbeiter die bearbeiteten Personendaten nur im Auftrag und zu Zwecken des Kunden und nicht zu eigenen Zwecken verwendet (Art. 10a Abs. 1 lit. a DSG Art. 9 Abs. 1 lit. a revDSG)? Wie sind die Eigentumsverhältnisse rund um die Daten geregelt? Wie teilen sich die Rollen und Verantwortlichkeiten zwischen Kunde und Auftragsbearbeiter auf? | M15 M16 | | | | |
| R5 | Ges | Grenzüberschreitende Bekanntgabe Sind geeignete Garantien (z.B. EU-Standardvertragsklauseln) implementiert, um bei Übermittlung von Personendaten in Länder ohne angemessenes Datenschutzniveau einen geeigneten Datenschutz zu gewährleisten (Art. 6 und Art. 10a Abs. 1 lit. a DSG Art. 16 und Art. 9 Abs. 1 lit. a revDSG)? | M15 | | | | |
| R6 | C Ges | Offenbarung geheimer Tatsachen Sind Informationen, die dem Amtsgeheimnis oder einem Berufsgeheimnis unterliegen, angemessen vor Klartextzugriffen des Auftragsbearbeiters oder Dritten geschützt (Art. 320 StGB, Art. 321 StGB)? Unterliegt die Datenverarbeitung durch den Auftragsbearbeiter einer angemessenen Vertraulichkeitsverpflichtung? | M2 M3 M4 M11 M12 M13 M15 M16 | | | | |
| R7 | Ges | Zugriff durch Behörden Bietet der Auftragsbearbeiter ausreichenden Einblick in seine Abläufe und Richtlinien bezüglich des staatlichen Zugriffs auf Daten, der dem Kunden eine informierte Entscheidung zu diesem Thema ermöglicht (Best Practice)? | M15 M16 | | | | |

| | | | |
|-----|------|--|-----|
| R8 | CIA | Mangelnde Governance | M1 |
| | Ges | Hat der Auftragsbearbeiter dem Kunden einen ausreichenden Einblick in das eigene interne Kontrollsystem (IKS) gegeben (Best Practice)? | M10 |
| | | Ist die Auditierung der Einhaltung der entsprechenden Sicherheitsverfahren und Sicherheitsrichtlinien sichergestellt und nachvollziehbar dokumentiert? | M15 |
| | | | M16 |
| R9 | I | Mangelndes Reporting | M7 |
| | Ges | Stellt der Auftragsbearbeiter zureichende Berichte über ausgelagerte Aktivitäten und Leistungen zur Verfügung (Best Practice)? Ist die Auditierung der Einhaltung der entsprechenden Sicherheitsverfahren und Sicherheitsrichtlinien sichergestellt und nachvollziehbar dokumentiert? | M15 |
| | | | M16 |
| R10 | C | Unerlaubter Zugang zu den Daten (KZ1) | M4 |
| | | Besteht Transparenz hinsichtlich der vom Auftragsbearbeiter getroffenen technischen und organisatorischen Massnahmen zum Schutz der Kundendaten vor nicht autorisiertem Zugang und physischem Zugriff, Verschlüsselung bei der Übertragung, Malware-Schutz, Vertraulichkeit, Authentifizierung sowie betrieblichen Richtlinien für dessen Mitarbeiter? | M5 |
| | | | M6 |
| | | | M15 |
| | | | M16 |
| R11 | C | Unerlaubter Zugriff auf die Daten (KZ2) | M5 |
| | | Ist der Auftragsbearbeiter in der Lage, Zugriffsrichtlinien zu Komponenten und Daten auszuweisen, und ist dabei sichtbar, dass angemessene Sicherheitsverfahren- und Sicherheitsrichtlinien angewendet werden? Bestehen Verfahren, welche den Zugriff auf Daten auch nach Ausfällen sicherstellt? | M6 |
| | | | M15 |
| | | | M16 |
| R12 | C, I | Unerlaubte Verwendung der Daten (KZ3) | M7 |
| | | Ist sichergestellt und ausgewiesen, dass der Auftragsbearbeiter entweder keinen Zugang zu den Daten des Kunden hat oder diese nur im Rahmen der beauftragten Auftragsbearbeitung einsehen kann? Ist eine Protokollierung allfälliger Datenzugriffe vorhanden? Existieren Vertraulichkeitsverpflichtungen im Rahmen der benötigten Funktionen seitens Auftragsbearbeiter? | M15 |
| R13 | C | Nicht konforme Löschung von Daten (KZ4) | M9 |
| | | Bestehen seitens Auftragsbearbeiter klare Richtlinien, wie eine Kündigung einer Subscription oder die Löschung von Daten durch den Kunden behandelt werden? Werden Hardware-Komponenten branchenüblich entsorgt? Sind die Daten portierbar? Ist sichergestellt, dass vertraglich ein Recht auf Anfragen zu diesem Thema besteht? | M15 |
| R14 | I | Gefährdete Integrität der Daten (KZ5) | M15 |
| | | Stellt der Auftragsbearbeiter sicher, dass dessen Mitarbeiter auf geeigneten Sicherheitsverfahren und Sicherheitsrichtlinien (z.B. Handling von Administrationssitzungen oder Passwörtern) geschult sind und diese aktiv befolgen? | M16 |
| R15 | A | Reduzierte Verfügbarkeit und Wiederherstellbarkeit der Daten (KZ6 & KZ7) | M9 |
| | | Stellt der Auftragsbearbeiter pro Service eine Dokumentation der SLA und der darauf basierenden Garantien zur Verfügung? Hat der Auftragsbearbeiter ein Geschäftsfortführungsmanagement implementiert? | M15 |
| | | Ist transparent, was bei der Abkündigung einzelner Services seitens Auftragsbearbeiter passiert? Sind auf der Basis der Plattform geeignete Wiederherstellungsverfahren und deren Prüfung implementiert? | M16 |
| | | Sind die Verantwortlichkeiten des Kunden in diesem Kontext klar? | |

Tabelle 3 – Risikoanalyse aufgrund gesetzlicher Grundlage und Grundlagen der Informationssicherheit

4 MASSNAHMEN UND KOMPONENTENBESCHRIEB

Dieses Kapitel gibt eine Auflistung und vertiefte Erklärung zu den möglichen Massnahmen, um den vorgängig aufgelisteten Risiken zu begegnen. Die Reihenfolge der Massnahmen sagt nichts über deren Priorität aus.

| Massnahmen-ID | Bereich | Massnahme | Massnahmen-Art |
|---------------|---------|--------------------------------------|---|
| M1 | C, I, A | ISO 27001 | Organisatorisch, Vertraglich |
| M2 | C, I, A | Azure Purview | Technisch, Organisatorisch |
| M3 | C, I, A | Azure Resource Tags | Technisch, Organisatorisch |
| M4 | C, I | Azure Key Vault | Technisch |
| M5 | C | Azure IAM (RBAC) | Technisch, Organisatorisch |
| M6 | C, I, A | Azure Policies | Technisch, Organisatorisch |
| M7 | A | Azure Monitor | Technisch |
| M8 | C | Compliance Manager für GDPR | Technisch, Organisatorisch, Vertraglich |
| M9 | C | Azure Data Subject Requests für GDPR | Technisch, Organisatorisch |
| M10 | C, I, A | Schulung im MPSCD | Organisatorisch |
| M11 | C | Kunden-Lockbox für Azure | Technisch, Organisatorisch |
| M12 | C, I, A | Azure Stack Hub | Technisch, Organisatorisch |
| M13 | C, I, A | Azure Stack HCI | Technisch, Organisatorisch |
| M14 | C, I, A | Azure Arc | Technisch, Organisatorisch |
| M15 | C | Vertragswerk | Vertraglich |
| M16 | C, I, A | Shared Responsibility Modell | Organisatorisch, Vertraglich |

Tabelle 4 – Massnahmenliste

4.1 M1 – AZURE BLUEPRINT – ISO 27001

Azure Blueprints stellen Vorlagen (Templates) dar, die Ressourcen, Policies und Berechtigungen zusammenfassen, welches als Ganzes angewendet und wiederverwendet werden können, um eine oder mehrere, standardisierte Basisumgebungen in Azure bereitzustellen.

Für das Swiss Public Sector Cloud Design wird ein bestehender Blueprint als Basis verwendet, welcher sich am ISO 27001 Sicherheitsstandard anlehnt und mit zielgerichteten Erweiterungen zur Begegnung der ermittelten Anforderungen ergänzt wird.

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Policy: Einschränkung von Cloud-Ressourcen zur Datenspeicherung und Bearbeitung in der Schweizer oder europäischen Azure Region
- Policy: Erzwingung von sicheren bzw. verschlüsselten Übertragungsprotokollen (TLS/SSL) der Kommunikation von Cloud-Ressourcen
- Policy: Erzwingung der zentralen Konsolidierung der Aktivitätsprotokolle (Logging) aller Ressourcen und Dienste

- Berechtigungen: Erstellung und Zuweisung von Berechtigungen auf Ressourcen und Dienste, um eine rollenbasierte, getrennte Zugriffssteuerung auf die Komponenten und Funktionen der Azure Umgebung zu realisieren
- Ressource: Erstellung eines Key Vault zur sicheren Speicherung von Verschlüsselungsschlüssel
- Ressource: Erstellung eines Log Analytics Workspace zur Aufbewahrung und allfälligen Auswertung von Aktivitätsprotokollen

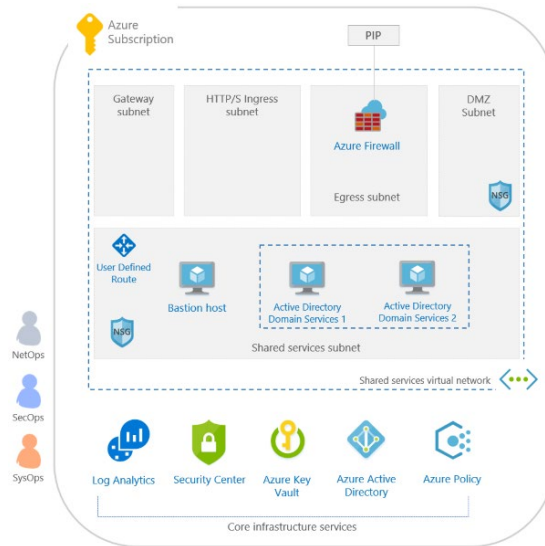


Abbildung 1 – ISO 27001 Blueprint 1

Weitere Komponenten können jederzeit dem Blueprint hinzugefügt oder ausserhalb als eigene Massnahmen implementiert werden.

4.2 M2 – AZURE PURVIEW

Das Azure Purview Werkzeug dient zur universellen und zentralen Erfassung aller gespeicherten Daten in der Cloud (nicht nur Azure) und on-Prem Ressourcen, um eine gesamtheitliche Datenlandkarte aller Informationen in Form von Metadaten zu erhalten. Hierbei wird ein Augenmerk auf Datenklassifizierung und Abstammung gelegt, um das Informationsvermögen beurteilen, eventuell nötige Massnahmen einleiten oder einfach Informationen finden zu können.

Der Informationsindex (Datenkatalog) wird über regelmässige Scans bekannter Ressourcen automatisch aufbereitet, wobei standardisierte und benutzerdefinierte Klassifizierungsregeln Anwendung finden, um bei der Datensuche als Filter zu dienen. Nebst der Klassifizierungsvermerken dient auch ein Begriffsglossar zur Markierung und Auffindung von Informationen.

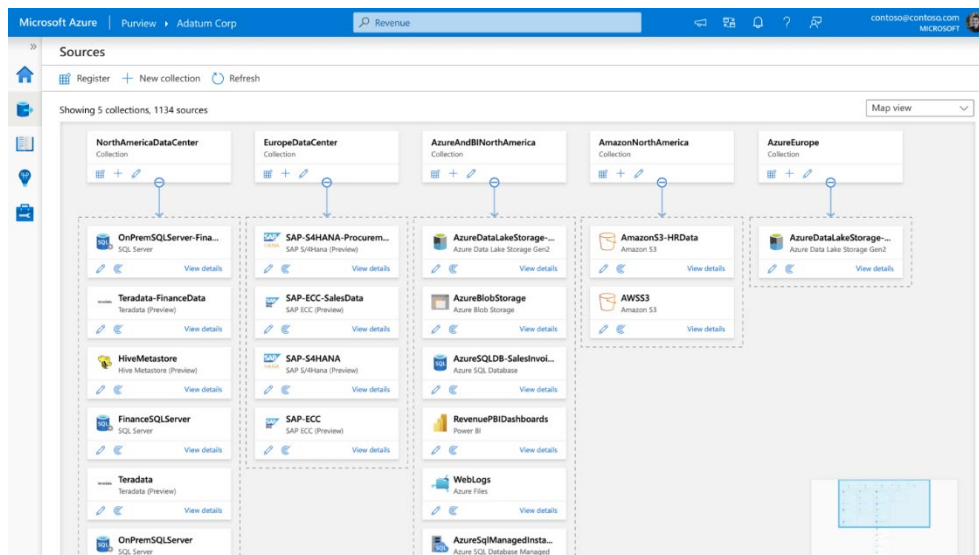


Abbildung 2 – Azure Purview

Über die standardisierte Apache Atlas Schnittstelle können auch Metadaten weiterer Quellen in den Datenkatalog importiert werden.

Azure Purview ist zur Klassifizierung und Indexierung der in Azure gespeicherten Daten und als Kontrollinstrument für Datenschutzbeauftragte wärmstens empfohlen.

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Identifizierung und Verwaltung von vertraulichen Daten

4.3 M3 – AZURE RESOURCES TAGS

Eine weitere universelle Möglichkeit, Ressourcen und ihre gespeicherten Daten zu klassifizieren, sind Resource Tags. Diese stellen frei definierbare Meta-Informationen dar, welche auf verschiedenen Ebenen der kontrollierten Azure Infrastruktur appliziert werden können. Diese können wiederum für verschiedene Zwecke ausgewertet werden. Azure Resource Tags sind ein Key Value Pair.

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Identifizierung und Verwaltung von vertraulichen Daten

4.4 M4 – AZURE KEY VAULT

Die Azure Plattform ist grundsätzlich durch Microsoft verschlüsselt, deren Schlüssel Sie verwalten. Azure Key Vault ist ein PaaS Dienst zur Einführung eigener Kundenschlüssel (a-/symmetrisch) zur Verschlüsselung der Kundendaten. Hierbei wird über explizite Berechtigungen von Dienstkonto von Ressourcen, wie z.B. Speicherkonto oder Azure SQL DB, zu den Schlüsseln gewährleistet, dass keine menschliche Interaktion mit den Chiffrierschlüsseln und Zertifikaten nötig ist und die Ver- und Entschlüsselung transparent geschieht.

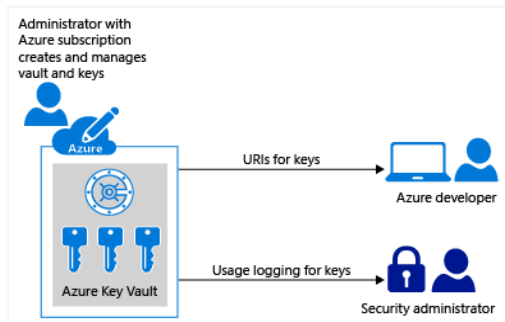


Abbildung 3 – Azure Key Vault

Verschlüsselungsschlüssel und Zertifikate sind in kundenkontrollierten Software-Instanzen von Key Vault gespeichert. Besteht die Anforderung, Verschlüsselungsschlüssel in dedizierten Hardware-Sicherheits-Modulen (HSM) zu speichern, oder gar in einem eigenen on-Prem HSM, kann dies mittels Key Vault Managed HSM realisiert werden.

Wenn in Ihrer Organisation eine der folgenden Anforderungen auftritt, kann Key Vault mit oder ohne Managed HSM zum Schutz von Kundendaten verwendet werden:

- Sie wollen auf jeden Fall sicherstellen, dass nur Sie geschützte Inhalte entschlüsseln können
- Sie möchten nicht, dass Microsoft Zugriff auf sehr sensible Daten hat
- Sie sind gesetzlich verpflichtet, Schlüssel innerhalb einer geografischen Grenze aufzubewahren

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Verschlüsselung von Sensitiven Daten

4.5 M5 – AZURE IAM (ROLE BASED ACCESS CONTROL RBAC)

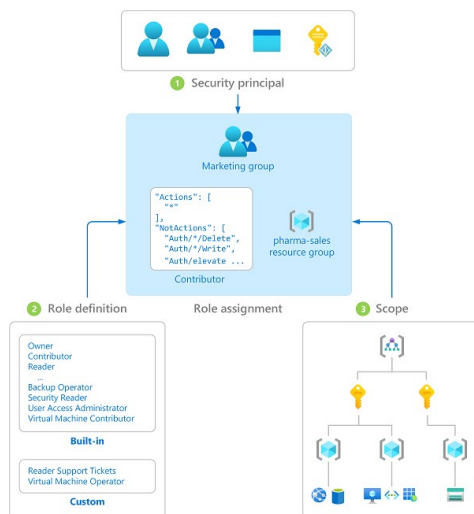


Abbildung 4 – Azure IAM (RBAC)

Die Aufgabentrennung und Zugangskontrolle zur Azure Plattform und ihren Dienst- und Applikationsressourcen wird über das integrierte, rollen-basierte Berechtigungssystem realisiert, wobei die Identitätenvorgängig durch Azure AD authentisiert werden. Azure bietet hierbei viele verschiedene, vordefinierte Berechtigungsrollen für Ressourcen und Plattformelemente, die den unterschiedlichen Identitätstypen zugewiesen werden können.

Das Berechtigungssystem erlaubt jedoch auch benutzerdefinierte Rollendefinitionen zu erstellen und zuzuweisen, falls die Standardrollen die nötigen Anforderungen nicht erfüllen.

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Zugriffsschutz auf Ressourcen

4.6 M6 – AZURE POLICIES

Azure Policies sind Richtlinien zur Regelung der Azure Infrastruktur, um organisatorische Anforderungen im grossen Rahmen zu prüfen oder gar zu erzwingen. Mittels Dashboards erlaubt es eine konsolidierte Übersicht der Regelkonformität zu erlangen, bietet aber auch die Möglichkeit zur Fokussierung der Konformitätssicht pro Ressource oder Richtlinie.

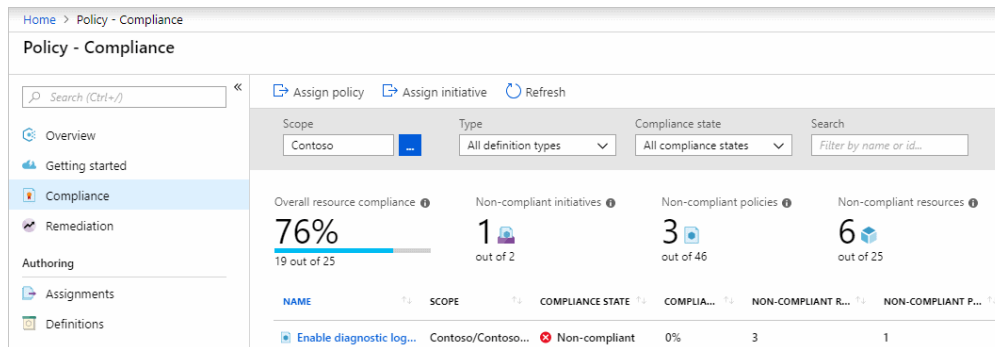


Abbildung 5 – Azure Policies

Policies eignen sich hervorragend, um z.B. folgende Anforderungen zu erzwingen oder kontrollieren:

- Bereitstellung von Ressourcen auf erlaubte Azure Regionen (z.B. CH, EU) zu beschränken
- Erzwingung zur verschlüsselten Datenübertragung mit vordefinierten Zertifikaten
- Erzwingung zur Datenverschlüsselung mit erlaubten Verschlüsselungsalgorithmen
- Erzwingung der zentralen Konsolidierung aller Aktivitätsprotokolle

Hierbei stehen viele vordefinierte Policies zum direkten Einsatz bereit, die falls nötig durch benutzerdefinierte Regeln ergänzt werden können.

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Einschränkung von Cloud-Ressourcen zur Datenspeicherung und Bearbeitung in der Schweizer oder europäischen Azure Region
- Erzwingung von sicheren bzw. verschlüsselten Übertragungsprotokollen (TLS/SSL) der Kommunikation von Cloud-Ressourcen
- Erzwingung der zentralen Konsolidierung der Aktivitätsprotokolle (Logging) aller Ressourcen und Dienste

4.7 M7 – AZURE MONITOR

Der Azure Monitor vereint alle Mittel zur Überwachung der Azure Plattform und der eingesetzten Dienste und Ressourcen in Bezug auf Verfügbarkeit, Leistung und Ereignisse. Es erlaubt Alarmierungen anhand von Schwellwerten und Ereignissen einzurichten, für welche zusätzliche Benachrichtigungen (z.B. Email, SMS) oder Automatismen ausgelöst werden, um den Betrieb aufrechterhalten zu können.

Mittels Workbooks lassen sich auch Monitoring Dashboards mit visuellen Indikatoren zur Verfügbarkeit und Leistung als auch Ereignisprotokollen erstellen.

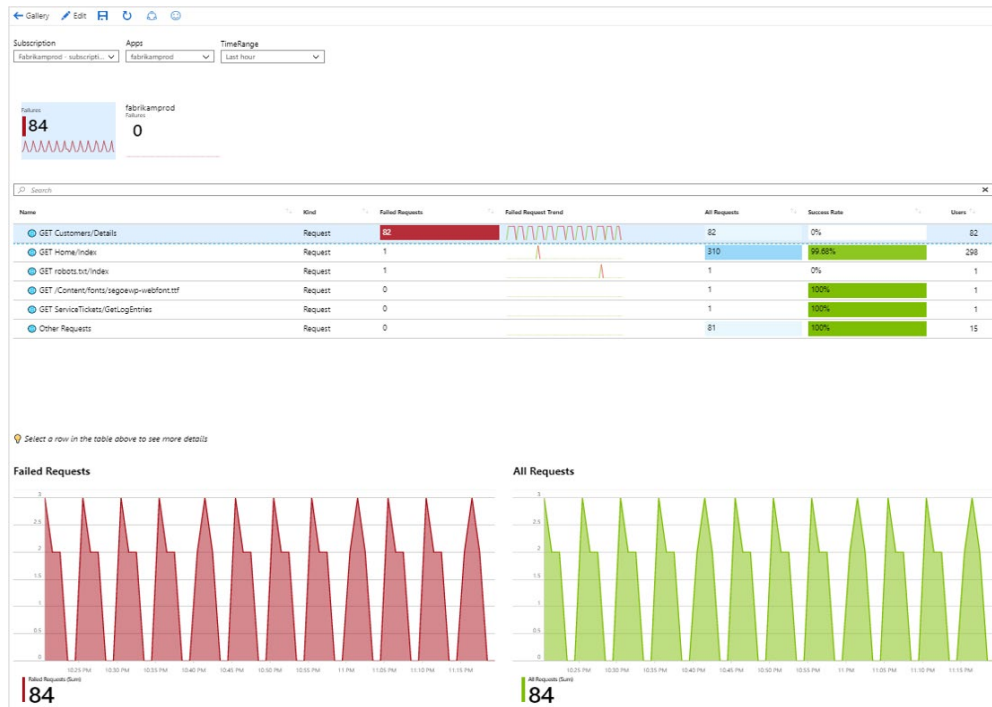


Abbildung 6 – Azure Monitor

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Übersicht der Verfügbarkeit von Ressourcen
- Alerts bei möglichen Störungen und Angriffen

4.8 M8 – MICROSOFT COMPLIANCE MANAGER FÜR GDPR / DSGVO

Der Compliance Manager ist ein Tool, mit dem Sie die Konformität ihrer Institution sowie die Azure-Implementation ihrer Institution mit der EU Datenschutz-Grundverordnung DSGVO / GDPR nachvollziehen und überprüfen können.

Der GDPR Compliance Manager bietet Ihnen zusätzliche Funktionen:

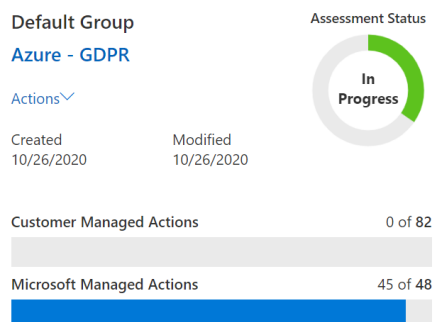


Abbildung 7 – Microsoft Compliance Manager für GDPR

- Kombinieren der Informationen, die Microsoft für Auditoren und Aufsichtsbehörden bereitstellt.
- Zuweisung von Compliance-Aktivitäten sowie deren Nachverfolgung und Aufzeichnung.
- Liefert eine Bewertung, die Ihnen dabei hilft, risiko-minimierende Controls nachzuverfolgen und zu priorisieren.
- Ist eine sichere Ablage für Dokumentationen und andere Artefakte.
- Erzeugt detaillierte Berichte, die Wirtschaftsprüfern, Aufsichtsbehörden oder anderen Beteiligten zur Verfügung gestellt werden können.

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Sicherstellung der Compliance gemäss DSGVO / GDPR

4.9 M9 – AZURE DATA SUBJECT REQUESTS FÜR GDPR / DSGVO

Die Datenschutz-Grundverordnung der Europäischen Union (DSGVO / GDPR) gibt betroffenen Personen das Recht, Einfluss auf personenbezogene Daten zu nehmen, die von einer Organisation über sie gesammelt wurden. Die GDPR gewährt den betroffenen Personen dazu bestimmte Rechte in Bezug auf ihre personenbezogenen Daten, wie z. B. Kopien von personenbezogenen Daten anzufordern, Korrekturen zu verlangen, die Verarbeitung einzuschränken, Daten zu löschen oder Daten in elektronischem Format zu erhalten, damit sie an einen anderen Verantwortlichen, bzw. Verarbeiter übertragen werden können. Ein formeller Antrag einer betroffenen Person an einen Datenverantwortlichen, Massnahmen bezüglich ihrer personenbezogenen Daten zu ergreifen, wird im Englischen als Data Subject Request oder DSR bezeichnet.

Das Azure Data Subject Requests for GDPR-Tool ermöglicht die Erfüllung von Anfragen der betroffenen Personen gemäss GDPR.

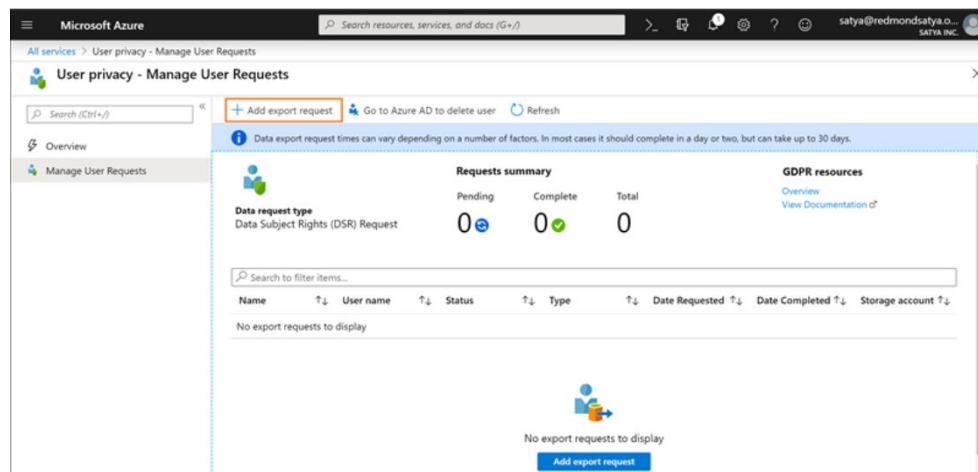


Abbildung 8 – Azure Data Subject Requests für GDPR

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Verwaltung (Zugriff, Aushändigung und Löschung) von GDPR Relevanten Daten

4.10 M10 – SCHULUNG FÜR MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Als weitere Basis zum effektiven Einsatz von Azure als Cloud-Plattform mit den vorgestellten Komponenten und Konzepten gilt es ebenfalls eine Schulung für alle damit betrauten Mitarbeiter durchzuführen.

- Einige Partner aus dem Microsoft Partner-Netzwerk bieten eine Einführung in das Microsoft Cloud Design.

| Grundlagen | Technologie | Betrieb |
|---|---|---|
| <ul style="list-style-type: none"> – Einführung Cloud Design – Datenschutzgesetz (DSG) – Informationsschutzverordnung (ISchV) – Informationssicherheit (ISO 27001) – Informationsklassifizierung | <ul style="list-style-type: none"> – Blueprints (Vorlagen) – Purview (Datenkatalog) – Policies (Richtlinien) – Key Vault (Verschlüsselung) – Monitor (Überwachung) – Kunden-Lockbox | <ul style="list-style-type: none"> – Blueprint Deployment – Konformitätsanalyse – Richtlinien erstellen – Umgebung einrichten – Kontinuierliche Überprüfung – Überwachung |

Abbildung 9 – Schulung in Microsoft Public Sector Cloud Design

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Vorbeugen von Fehlmanipulationen
- Sicherstellung der betrieblichen Kontinuität
- Steigerung Verständnis der IT-Abteilungen für die Technologien, Risiken und Möglichkeiten

4.11 M11 – KUNDEN-LOCKBOX FÜR AZURE

Die Kunden (Customer) Lockbox für Microsoft Azure ermöglicht es Ihnen als Kunde, eine Anfrage von Microsoft für den Zugriff auf Kundendaten zu überprüfen und zu genehmigen/abzulehnen. Sie wird in Fällen verwendet, in denen ein Microsoft-Techniker während einer Support-Anfrage Zugriff auf Kundendaten benötigt.

So kann z. B. beurteilt werden, ob Informationen, die während einer Supportanfrage weitergegeben werden sollen, vertraulich sind oder nicht, und ob sie eingesehen werden dürfen oder nicht.

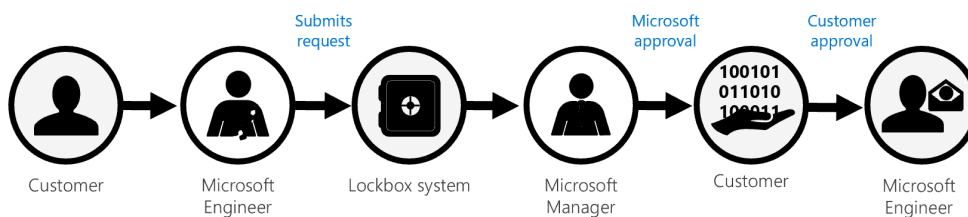


Abbildung 10 – Kunden-Lockbox

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Vertraulichkeit von Personendaten wahren

4.12 M12 – AZURE STACK HUB

Azure Stack Hub ist Ihre eigene private Azure-Cloud, die Sie ganz oder teilweise getrennt vom Internet betreiben können. Azure Stack Hub ist Teil des Azure Stack-Portfolios und erweitert Azure, sodass Sie Apps in einer On-Premises-Umgebung ausführen und Azure-Dienste in Ihrem Rechenzentrum bereitstellen können. Viele Unternehmen führen eine digitale Transformation durch und stellen fest, dass sie den Prozess beschleunigen können, indem sie Public-Cloud-Dienste nutzen, um moderne Architekturen zu erstellen und Legacy-Apps zu aktualisieren. Einige Workloads müssen jedoch lokal bleiben - zum Beispiel wegen unterschiedlichen technischen und rechtlichen Anforderungen. Mit Azure Stack Hub können Sie zum Beispiel sensible, als geheim eingestufte Daten speichern.



Abbildung 11 – Azure Stack Hub

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Datenhaltung in den eigenen Rechenzentren

4.13 M13 – AZURE STACK HCI

Azure Stack HCI erfüllt das gleiche Ziel wie schon Azure Stack Hub: Daten, welche nicht in die Cloud migriert werden dürfen, OnPremises zu betreiben.

Azure Stack HCI ist eine standardisierte, von Hardware Herstellern und Microsoft zusammen entwickelte sowie zertifizierte Hyper-converged Virtualisierungsplattform, auf welcher virtuelle Server betrieben werden können. Folgende Infrastruktur Dienste werden damit bereitgestellt:

- Azure Stack HCI-Betriebssystem
- Überprüfte Hardware von einem OEM-Partner
- Azure-Hybriddienste
- Windows Admin Center
- Hyper-V-basierte VMs
- Auf direkten Storage Spaces direkt basierender virtualisierter Speicher
- SDN-basiertes virtualisiertes Netzwerk mit Netzwerkcontroller (optional)

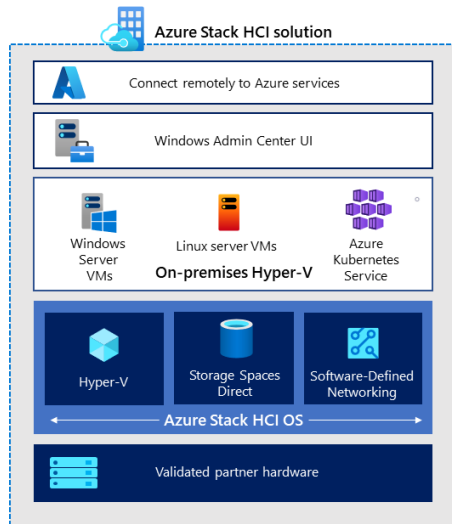


Abbildung 12 – Azure HCI

Ausserdem können auch zusätzliche Azure-Hybriddienste genutzt werden:

- Azure Site Recovery, zur Erzielung von Hochverfügbarkeit und Notfallwiederherstellung als Dienst (Disaster-Recovery-as-a-Service, DRaaS)
- Azure Monitor, ein zentraler Hub, in dem Sie die Aktivität Ihrer Apps, Netzwerke und Infrastrukturen überwachen können – mittels erweiterter KI-Analysen
- Cloud Witness, um Azure als einfache Entscheidungshilfe für ein Clusterquorum zu verwenden
- Azure Backup, für den Schutz von Daten durch Speicherung an anderen Standorten und den Schutz vor Ransomware
- Azure-Update Management, für die Bewertung und Bereitstellung von Updates für Windows-VMs, die in Azure und lokal ausgeführt werden
- Azure-Network Adapter, zum Verbinden lokaler Ressourcen mit Ihren VMs in Azure über ein Point-to-Site-VPN
- Azure-File Sync, zum Synchronisieren Ihres Dateiservers mit der Cloud

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Datenhaltung in den eigenen Rechenzentren

4.14 M14 – AZURE ARC

Azure Arc bietet eine konsistente Verwaltungsplattform für verschiedene Public Clouds und die lokale Umgebung und vereinfacht so die Governance und Verwaltung. Mit Azure Arc können folgende Aktionen durchgeführt werden:

- Die gesamte Umgebung kann über eine zentralisierte Benutzeroberfläche verwaltet werden, indem die vorhandenen Ressourcen (Ressourcen, die aus Azure stammen, lokale Ressourcen oder jene aus anderen Clouds) in Azure Resource Manager projiziert werden
- Verwaltung von virtuellen Computern, Kubernetes-Clustern und Datenbanken so, als würden sie in Azure ausgeführt
- Implementieren einer konsistenten Bestands-, Verwaltungs-, Governance- und Sicherheitslösung für die Server in Ihrer gesamten Umgebung
- Konfigurieren von Azure-VM-Erweiterungen für die Verwendung von Azure-Verwaltungsdiensten zur Überwachung, zum Schutz und zur Aktualisierung Ihrer Server

Mit Azure Stack HCI kann von folgenden Azure Services profitiert werden:

- Überwachung: Zeigen Sie Ihre gesamten Azure Stack HCI-Cluster in einer zentralen globalen Ansicht an, in der Sie sie nach Ressourcengruppe gruppieren und markieren können.
- Abrechnung: Bezahlen Sie Azure Stack HCI über Ihre Azure-Subscription.

- Einheitliche Betrachtung Ihrer Azure Arc-fähigen Ressourcen bei Verwendung von Azure-Portal, Azure CLI, Azure PowerShell oder Azure-REST-API

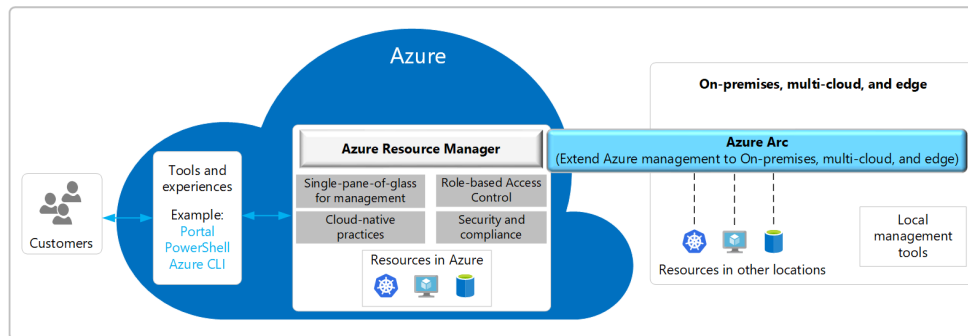


Abbildung 13 – Azure Arc

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Identifizierung und Verwaltung von vertraulichen Daten
- Eindämmung der Sicherheitslücken durch Updates und Virens Scanner für Workloads in der Cloud und onPremises
- Einheitliche Governance über alle verwendeten Ressourcen hinweg
- Sicherstellung der Compliance der Ressourcen durch zentrales Management

4.15 M15 – VERTRAGSWERK

Um das notwendige Verständnis und die Einsicht zu erlangen, die den Ausgangspunkt für den Nachweis dieser Kontrolle bildet, ist es unerlässlich, die Gesamtstruktur der Microsoft Cloud-Vereinbarungen, der Dokumentation, der Anleitungen und nicht zuletzt der Zertifizierungen und Auditberichte zu kennen. Hier bietet das sog. Microsoft Assurance Framework den notwendigen Überblick und eine Anleitung für den zu befolgenden Prüfprozess:

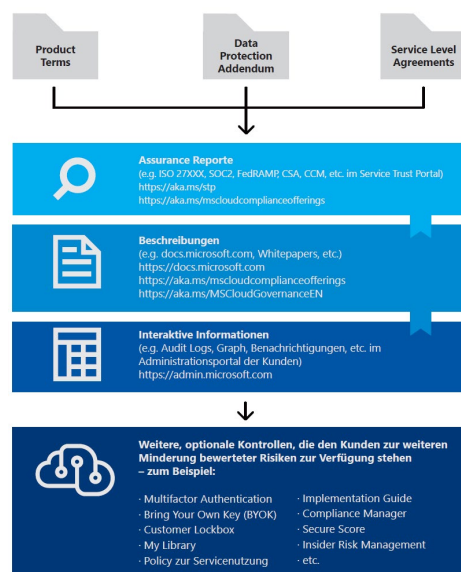


Abbildung 14 – Microsoft Assurance Framework

- Die oberste Ebene bildet das abzuschließende **Vertragswerk mit Microsoft**. Dies beinhaltet u.a. die **License Terms**, in der die Datenverarbeitungsvereinbarung (für Microsoft Cloud genannt **Data Protection Addendum**) enthalten sind.
- Die im Vertragswerk festgelegten vertraglichen Pflichten von Microsoft können anhand der Dokumente der zweiten Ebene, den sog. **Assurance Reports**, überprüft werden. Kunden können auf sämtliche **Audit-Berichte von Drittanbietern, Zertifikate zur Einhaltung von Standards, SOA** usw. zugreifen.
- Die dritte Ebene umfasst weiterführende beschreibende Dokumentationen, in welchen Microsoft **Anleitungen und Beschreibungen** zu bestimmten Funktionen, Features, Prozessen und ähnlichem zur Verfügung stellt. Ebenfalls erhältlich sind eine Reihe von themen- oder sektorspezifischen **White Papers** wie bspw. auch dieses Dokument.

- Schliesslich haben Kunden Zugriff auf fortlaufende Dokumentationen und Informationen speziell zur Nutzung von Microsoft Cloud-Diensten, die über ein individuelles **Cloud-Service Verwaltungsportal** zur Verfügung stehen.

Für alle diese vier Ebenen gibt es zusätzliche Funktionen, Dienste und Prozesse, die für den einzelnen Kunden implementiert werden können. Diese können auf der Grundlage der allgemeinen Risikobewertung der Lösung und der Datenflüsse eingesetzt werden und können somit in einen Mitigationsplan in Bezug auf die identifizierten Risiken aufgenommen werden, die der Kunde mindern möchte. In der obigen Abbildung sind einige der häufigsten Massnahmen im Kasten rechts dargestellt und werden z.T. später in diesem Dokument beschrieben.

Das Microsoft Assurance Framework spielt damit eine entscheidende Rolle im Zusammenhang mit der Erstellung von Kontrollen beim Kunden. Der Zusammenhang ist im folgenden Prozessmodell dargestellt:

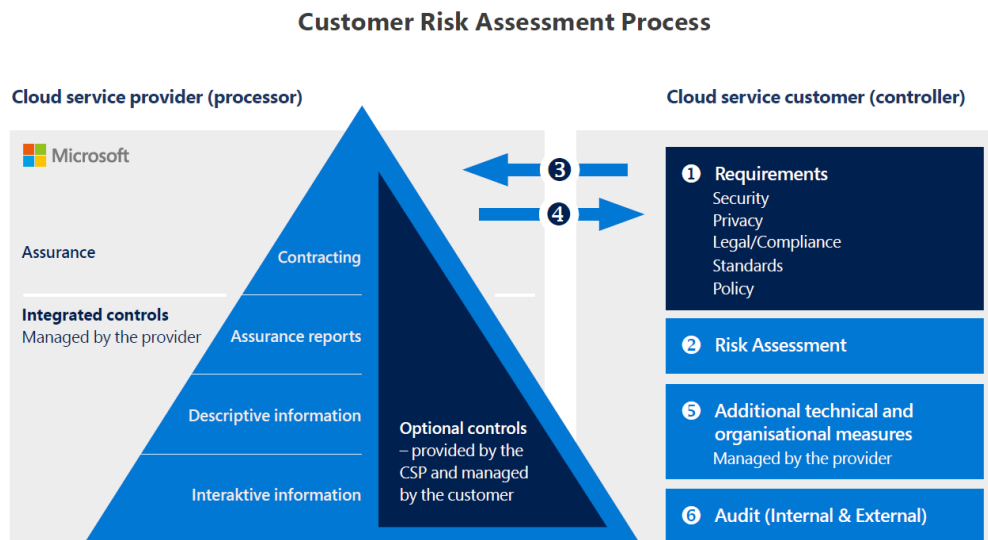


Abbildung 15 – Beziehung der Cloud-Governance des Kunden und dem Microsoft Assurance Framework

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Sicherstellung der Compliance
- Einschränkungen von Risiken durch Richtlinien



4.16 M16 – SHARED RESPONSIBILITY MODEL

Die Ausprägung resp. die Organisation der Kontrolle bzw. den «Mix» und das Zusammenspiel der verschiedenen Instrumente zur Ausübung der Kontrolle unterscheidet sich je nach Integrationstiefe der beigezogenen Cloud-Lösungen. Dies widerspiegelt sich auch in der Verteilung der Verantwortung und der Kosten für die Etablierung eines angemessenen Schutzes gegen gewisse Risiken (insb. Datenschutz und –sicherheit).

In einer Cloud-Umgebung wird, im Gegensatz zu einer lokalen IT-Infrastruktur, die Verantwortung für die

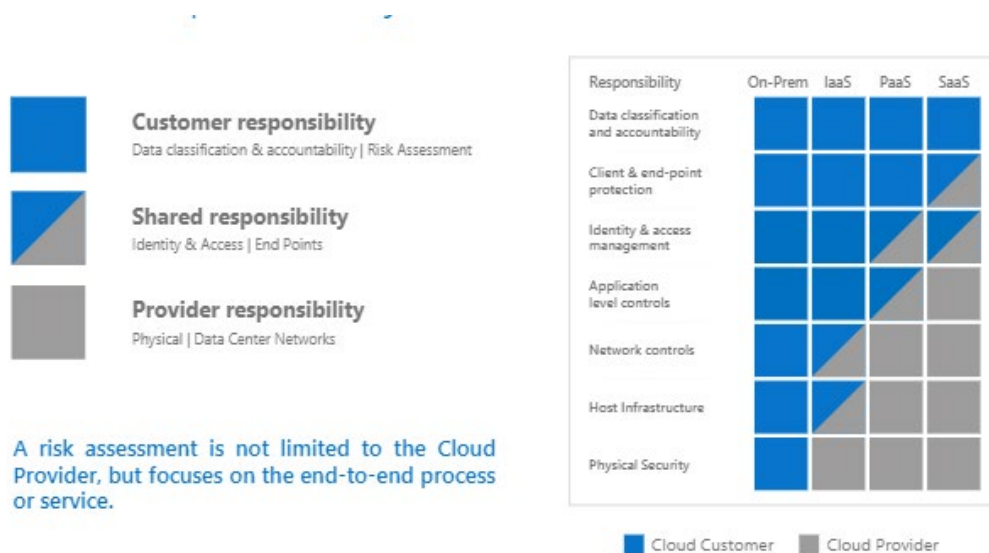


Abbildung 16 – Shared Responsibility Modell

Implementierung und Pflege von Sicherheitskontrollen für IT-Anwendungen zwischen dem Kunden und dem Cloud-Anbieter geteilt. Dies gleicht einem klassischen Outsourcing-Szenario. Die endgültige Verantwortung für die verarbeiteten Daten verbleibt jedoch stets beim Kunden.

Grundsätzlich folgen moderne Cloud-Lösungen einem geteilten Verantwortlichkeitsmodell («shared responsibility model»). Dieses unterteilt die Verantwortung zwischen dem Kunden und dem Cloud-Anbieter entlang der Virtualisierungsgrenzen, so dass jeweils primär eine Partei für einen bestimmten Aspekt verantwortlich ist.

Bei Cloud-Lösungen findet eine gewisse Verlagerung der Kontrollfunktion dahingehend statt, dass die organisatorischen/operationellen Aspekte der Kontrolle an Bedeutung zunehmen. Da beispielsweise eine Behörde in einem Cloud-Umfeld nur beschränkt selber die Möglichkeit hat, technische Massnahmen gegen unerlaubten Datenzugriff umzusetzen (weil der Cloud-Anbieter die diesbezügliche Technik stellt), hat die Behörde ihre Verantwortung durch geeignete andere Massnahmen wahrzunehmen. Nebst einer sorgfältigen Evaluation des Cloud-Anbieters könnte beispielsweise ein regelmässiges Monitoring der Wirksamkeit des vom Anbieter bereitgestellten Datenschutzes eine zweckmässige Massnahme zur Sicherstellung der Kontrolle sein (z.B. laufende Überwachung von Zugriffen und Zugriffsversuchen über die entsprechende Auswertung von Ereignisprotokollen).

Zur Gewährleistung der Qualität des vom Cloud-Provider verantworteten Teils des «Shared responsibility Model» hat Microsoft für Azure zahlreiche sicherheits-, industrie- und länderspezifische Audits durchgeführt, um die Security Compliance im Betrieb der Cloud-Plattform durch Dritte zu zertifizieren. Die Sicherheitsstandards umfassen unter anderem ISO und SOC, deren Auditberichte im Service Trust Portal¹⁸ abrufbar sind.

Diese Massnahme kann eingesetzt werden, um folgende Punkte umzusetzen, welche identifizierten Risiken begegnen:

- Verantwortlichkeiten zwischen Provider und Kunde regeln
- Unterstützung der Risikoeinschätzung

¹⁸ <https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide>

APPENDIX:


WICHTIGE VERTRAGSGRUNDLAGEN UND LINKS

Die folgende Tabelle listet die wichtigsten Informationsquellen für Transparenz im Zusammenhang mit diesem Dokument auf.

| Dokument oder Themenbereich | Verweise |
|--|---|
| Einstiegsseite Datenschutzbestimmungen | https://privacy.microsoft.com/de-de/privacystatement |
| Nachtrag zum Datenschutz für Produkte und Dienstleistungen (Data Protection Addendum, DPA), September 2021 | https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&year=2021 |
| Universelle Lizenzbestimmungen für Onlinedienste | https://www.microsoft.com/licensing/terms/product/ForOnlineServices |
| Microsoft Business and Services Agreement (MBSA) | https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4f5aA |
| Technische Dokumentationen der Azure Services | https://docs.microsoft.com/de-ch/ |
| Microsoft Trust Center (Compliance & Security Dokumentationen) | https://www.microsoft.com/de-ch/trust-center |
| SLA-Dokumentation aller Azure-Services | https://azure.microsoft.com/de-de/support/legal/sla/summary/ |

Tabelle 5 – Zusammenstellung wichtiger Informationsquellen





Danke
Merci
Grazie
Engraziel