



MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Microsoft 365 im öffentlichen Sektor der Schweiz

Version 1.1

Inhalt

1	Einleitung zum Microsoft Public Sector Cloud Design	4
1.1	Kontrolle von Daten als Kernthema.....	4
2	Rechtliche Herausforderungen beim Cloud Design	5
2.1	Übersicht.....	5
2.1.1	Cloud Computing als eigener Auslagerungssachverhalt	5
2.1.2	Ausland.....	5
2.2	Gesetzliche Regelungen.....	6
2.2.1	Allgemeines.....	6
2.2.2	Die gängigsten Vorgaben im Einzelnen.....	6
2.2.2.1	Vertragliche Vereinbarung.....	6
2.2.2.2	Bearbeitung nach Weisung und im Interesse des öffentlichen Organs	7
2.2.2.3	Einbezug weiterer Datenbearbeiter.....	7
2.2.2.4	Datensicherheit.....	7
2.2.2.5	Auslandsbezüge	8
2.2.2.6	Behördenzugriffe	9
2.2.2.7	Kritische Daten.....	10
2.3	Informationsschutzverordnung (ISchV).....	11
3	Kontrollziele und Risiken.....	12
3.1	Kontrollziele	12
3.2	Risikoanalyse.....	13
4	Massnahmen und Komponentenbeschrieb.....	16
4.1	M1 – ISO 27001	16
4.2	M2 – Microsoft Secure Score & Security Compliance Toolkit.....	17
4.3	M3 – Microsoft Purview Information Protection	18
4.4	M4 – Datenschutz-Folgenabschätzungen (DSFA).....	19
4.5	M5 – Microsoft 365 IAM & Privileged Access Management.....	20
4.6	M6 – Microsoft Purview Compliance Manager	21
4.7	M7 – Data Subject Request	22
4.8	M8 – Microsoft Public Sector Cloud Design Schulung	22
4.9	M9 – Microsoft Purview Customer Lockbox.....	23
4.10	M10 – Verschlüsselung	24
4.11	M11 – Microsoft 365 Hybrid mit Exchange und SharePoint	25
4.12	M12 – Vertragswerk	26
4.13	M13 – Shared Responsibility Model.....	27
4.14	M14 – Privacy Management für Microsoft 365.....	28
	Appendix : Wichtige Vertragsgrundlagen und Links.....	30

Tabellen

Tabelle 1 – Matrix Klassifizierungsstufen und Massnahmen nach ISchV	11
Tabelle 2 – Kontrollziele der Informationssicherheit	13
Tabelle 3 – Risikoanalyse auf der Grundlage von Rechtsgrundlagen und Grundlagen der Informationssicherheit.....	15
Tabelle 4 – Liste der Massnahmen.....	16
Tabelle 5 – Zusammenstellung wichtiger Informationsquellen	30

Abbildungen

Abbildung 1 – Microsoft Service Trust Portal.....	17
Abbildung 2 – Microsoft Secure Score.....	18
Abbildung 3 – Microsoft Purview Information Protection.....	19
Abbildung 4 – Vorlage für Datenschutz-Folgenabschätzungen (DPIA)	20
Abbildung 5 – Privileged Access Management für Microsoft 365	20
Abbildung 6 – Microsoft 365 Purview Compliance Manager.....	21
Abbildung 7 – Microsoft 365 Priva Dashboard.....	22
Abbildung 8 – Struktur der Microsoft 365 Public Sector Cloud Design Schulung.....	22
Abbildung 9 – Microsoft Public Sector Cloud Design Schulung.....	23
Abbildung 10 – Customer Lockbox Prozess.....	23
Abbildung 11 – Typische Datenlandschaft einer Organisation.....	24
Abbildung 12 – Microsoft 365 Hybrid-Konfiguration für Exchange	25
Abbildung 13 – Microsoft Assurance Framework.....	26
Abbildung 14 – Customer Risk Assessment Prozess.....	27
Abbildung 15 – Shared Responsibility Model	28
Abbildung 16 – Dashboard zur Datenschutzverwaltung für Microsoft 365	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.

© (2022) 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.

1 EINLEITUNG ZUM MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Mit dem Aufkommen der modernen Kommunikation und Zusammenarbeit und dem so genannten «New-Work», wurden «Hybrid»- und «Remotework» zu einem entscheidenden Faktor für den Erfolg jeder Behörde. Mit der Nutzung von Produktivitätslösungen wie Microsoft 365 und insbesondere Microsoft Teams, sind Cloud-Lösungen inzwischen weit verbreitet. Diese leicht zugänglichen Dienste werden auch in Behörden immer beliebter.

Während die Vorteile auf der Hand liegen, gibt es auch Herausforderungen, denen sich die Behörden stellen müssen: In einer «Cloud-First»-Welt liegen die Daten beim Cloud-Anbieter, bleiben aber unter der Kontrolle der Behörde. Man spricht davon, dass die sog. Datenverarbeitung an den Cloud-Anbieter «ausgelagert» wird. Um die Kontrolle über die ausgelagerte Datenverarbeitung zu gewährleisten, müssen sich Kunden mit den Standards und allgemeinen Vorschriften des Cloud-Anbieters auseinandersetzen, insbesondere in Bezug auf die Informationssicherheit.

Daher müssen Kunden des öffentlichen Sektors wissen, welche Hilfestellung Microsoft als Cloud-Service-Provider bieten kann, wenn sich diese für die Nutzung von Microsoft 365 Online-Services entscheiden. Die daraus resultierenden Risiken müssen Kunden aus dem Behördenumfeld identifizieren, und verstehen, welche vertraglichen, organisatorischen und technischen Massnahmen Microsoft bereitstellt, damit die Online-Services sicher genutzt werden können.

Dieses Dokument gibt Kunden einen Überblick über die wesentlichen Kontrollziele und konkreten Massnahmen auf Basis der Microsoft 365 Technologien, mit Fokus auf den öffentlichen Sektor.

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 vernünftigem 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 Microsoft 365 Services generell immer verschlüsselt ist) oder deren Verwertung durch einen unbefugten Dritten die betroffenen Personen empfindlich treffen könnte (z.B. Amtsgeheimnisse).

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 4.12).

¹ <https://www.news.admin.ch/newsd/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 selbstständig 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 Bezug von Unterauftragsbearbeitern etc.). Die meisten Kantone stellen diesbezüglich jedoch keine besonderen, über die Vorgaben 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 grössererem 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 DSG sowie verschiedene kantonale Gesetzgebungen enthalten diesbezüglich Bestimmungen, dass die Daten nur so bearbeiten 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 wie in den Datenschutzbestimmungen beschrieben und eingeschränkt verarbeiten, (a) um dem Kunden die Produkte und Services in Übereinstimmung mit den dokumentierten Anweisungen des Kunden zur Verfügung zu stellen, und (b) für die Geschäftstätigkeiten von Microsoft, die mit der Bereitstellung der Produkte und Services an den Kunden verbunden sind. 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 gegenüber Microsoft in Bezug auf die Verarbeitung personenbezogener Daten 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 der Unterauftragnehmer, 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 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 Stufen, «Time-Boxing» 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 4.9).

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.

³ Datenschutznachtrag zu den Produkten und Services von Microsoft: <https://aka.ms/dpa>

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

Microsoft verwendet in den Onlinediensten zahlreiche Verschlüsselungen auf verschiedenen 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, womit ein physikalischer Zugriff auf die Daten ausgeschlossen ist. 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 ermöglichen die Onlinedienste dem Cloud-Kunden verschiedene 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 Center 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.

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

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



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.⁷

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-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 auszustalten, dass die Kernkundendaten innerhalb Europas 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 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 anzufechten.¹³

7 <https://aka.ms/dpa>, «Datenübermittlungen»

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/>

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.

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.

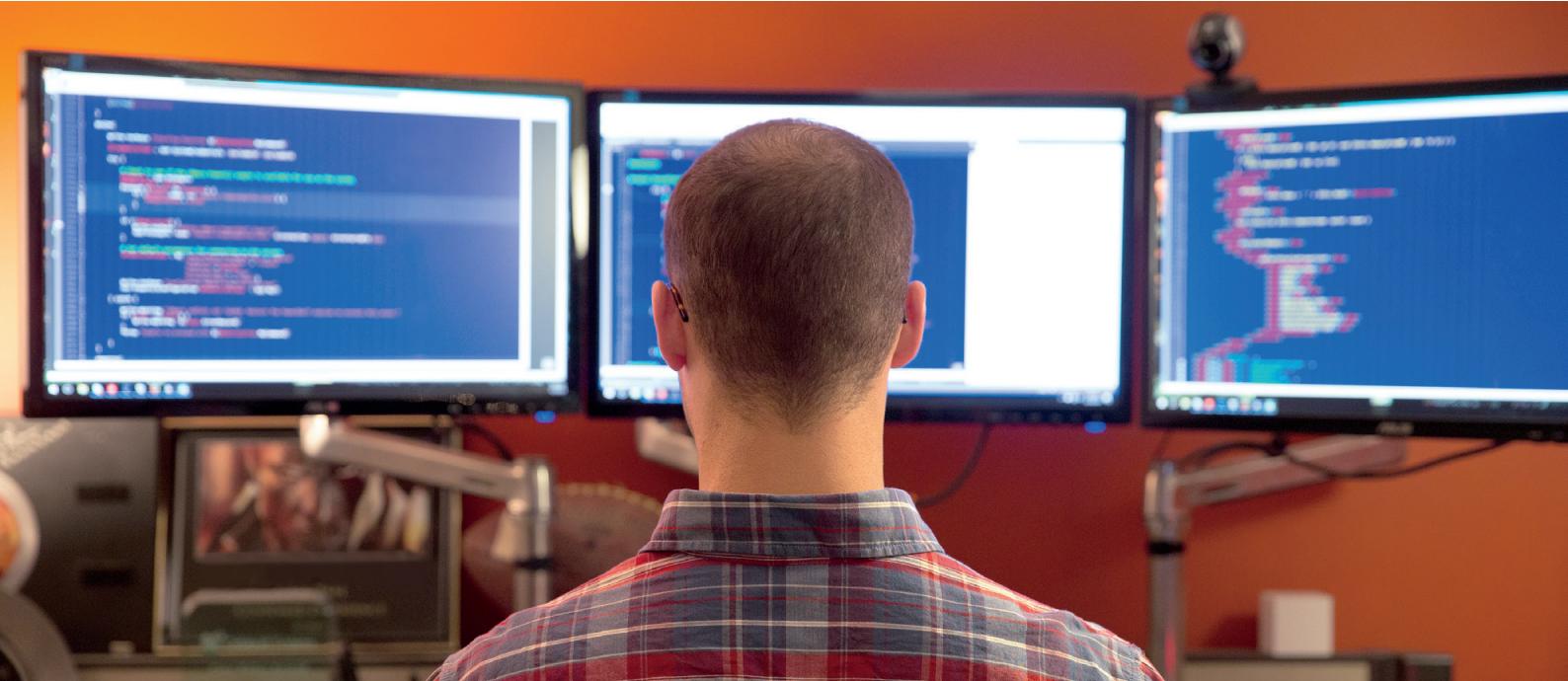
Zu beachten ist weiter, dass der zahlenmässige Unterschied zwischen Anfragen für Verbraucherkonten und Unternehmenskonten auch die formalen Richtlinien¹⁵ der Abteilung für Computerkriminalität und geistiges Eigentum des US-Justizministeriums wiederspiegelt, die Staatsanwälten rät, sich direkt an Unternehmen 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.

14 <https://aka.ms/mslrr>

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 zu Informationen, dem Grad der Schutzwürdigkeit entsprechend. Dabei werden letztlich Massnahmen vorgeschlagen oder können davon abgeleitet werden. 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 Arbeitsplatzsystemen oder entfernbaren Datenträgern	Nur auf bewilligten Mitteln oder verschlüsselt auf Arbeitsplatzsystemen oder entfernbaren Datenträgern
Datenübertragung	Geschützter übertragungsweg (z.B. Bundesnetz)	Verschlüsselung oder geschützter Übertragungsweg	Verschlüsselung oder geschützter Über- tragungsweg
Bearbeitung mit Informatikmitteln	Zulässig	Nur mit von der Koordina- tionsstelle bewilligten Mitteln (Ausnahme: Armee) und unter Verwendung von Sicherheitssoftware gemäß Bundesstandard	Nur mit von der Koordina- tionsstelle bewilligten Mitteln und unter Verwendung von Sicherheitssoftware gemäß Bundesstandard
Mitnahme ab dauerndem Standort	Zulässig	Eingeschränkt zulässig	Eingeschränkt zulässig
Rückzug und Rück- gabepflicht	Keine	Zwingend	Zwingend
Vernichtung bzw. Lösichung	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 INTERN klassifizierte Informationen bearbeitet

3 KONTROLLZIELE UND RISIKEN

Wie auch in anderen Bereichen, gibt es 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 und Kontrollziele verfolgen:

– Geheime Daten

Geheime Daten werden in einem ersten Schritt nicht in der Cloud abgelegt, sondern lokal gespeichert. Um dabei soweit wie möglich von den Funktionen von Microsofts 365 zu profitieren, bietet eine hybride Bereitstellung für Exchange und SharePoint ein durchgängiges Benutzererlebnis, während gleichzeitig der höchstmögliche Datenschutz gewährleistet wird.

– Vertrauliche Daten

Vertrauliche Daten dürfen verschlüsselt in der Cloud gespeichert werden. Hierfür eignet sich Microsoft Purview Information Protection (MIP), entweder mit eigenem Schlüssel (BYOK) oder unter Verwendung von zwei Schlüsseln – einer in Azure und einer lokal beim Kunden (Double Key Encryption).

– Recht auf Auskunft des Betroffenen

Unternehmen müssen unter Umständen auf formelle Anfragen einer betroffenen Person reagieren. Microsoft 365 bietet die notwendigen Werkzeuge, um Kopien personenbezogener Daten bereitzustellen und um Korrekturen, Übertragungen oder Löschungen der personenbezogenen Daten des Betroffenen zu beantragen.

Es wird in den folgenden Kapiteln darauf verzichtet, Massnahmen spezifischen 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 DSG, 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	Lösungskontrolle Ist sichergestellt, dass der Unterauftragsbearbeiter die Daten löscht, wenn die Auslagerung endet?	Art. 10a Abs. 1 lit. a DSG 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 DSG 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 DSG 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 DSG 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	Risikoauswirkung 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 Bezug neuer Unterauftragsbearbeitern dem Kunden ein Widerspruchsrecht gewährt (Art. 9 Abs. 3 revDSG)? Unterstehen die Unterauftragsbearbeiter denselben gesetzlichen und regulatorischen Grundlagen wie der Auftragsbearbeiter?	M12			
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?	M2 M4 M6 M8 M12 M14			
R3	Ges	Nicht gemeldete Datensicherheits-Verletzung Ist sichergestellt, dass der Auftragsbearbeiter Datensicherheits-Verletzungen 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?	M1 M2 M12 M13			
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?	M12 M13			
R5	Law	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)?	M11 M12			
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 M9 M10 M12 M13			
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)?	M4 M12 M13 M14			

R8	CIA	Mangelnde Governance	<u>M1</u>
	Ges	Hat der Auftragsbearbeiter dem Kunden einen ausreichenden Einblick in das eigene interne Kontrollsysteem (IKS) gegeben (Best Practice)? Ist die Auditierung der Einhaltung der entsprechenden Sicherheitsverfahren und Sicherheitsrichtlinien sichergestellt und nachvollziehbar dokumentiert?	<u>M4</u> <u>M8</u> <u>M12</u> <u>M13</u> <u>M14</u>
R9	I	Mangelndes Reporting	<u>M4</u>
	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?	<u>M12</u> <u>M13</u> <u>M14</u>
R10	C	Unerlaubter Zugang zu den Daten (KZ1)	<u>M3</u>
		Besteht Transparenz hinsichtlich der vom Auftragsbearbeiter getroffenen technischen und organisatorischen Massnahmen zum Schutz der Kundendaten vor nicht autorisiertem Zugang und physikalem Zugriff; Verschlüsselung bei der Übertragung, Malwarschutz, Vertraulichkeit, Authentifizierung sowie betrieblichen Richtlinien für dessen Mitarbeiter?	<u>M9</u> <u>M10</u> <u>M12</u> <u>M13</u>
R11	C	Unerlaubter Zugriff auf die Daten (KZ2)	<u>M3</u>
		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?	<u>M5</u> <u>M12</u> <u>M13</u>
R12	C, I	Unerlaubte Verwendung der Daten (KZ3)	<u>M9</u>
		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?	<u>M10</u> <u>M11</u> <u>M12</u>
R13	C	Nicht konforme Löschung von Daten (KZ4)	<u>M1</u>
		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?	<u>M6</u> <u>M7</u> <u>M12</u>
R14	I	Gefährdete Integrität der Daten (KZ5)	<u>M1</u>
		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?	<u>M12</u> <u>M13</u>
R15	A	Reduzierte Verfügbarkeit und Wiederherstellbarkeit der Daten (KZ6 & KZ7)	<u>M7</u>
		Stellt der Auftragsbearbeiter pro Service eine Dokumentation der SLA und der darauf basierenden Garantien zur Verfügung? Hat der Auftragsbearbeiter ein Geschäftsfortführungsmanagement implementiert? Ist transparent, was bei der Abkündigung einzelner Services seitens Auftragsbearbeiter passiert? Sind auf der Basis der Plattform geeignete Wiederherstellungsverfahren und deren Prüfung implementiert? Sind die Verantwortlichkeiten des Kunden in diesem Kontext klar?	<u>M12</u> <u>M13</u>

Tabelle 3 – Risikoanalyse auf der Grundlage von Rechtsgrundlagen 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	Microsoft Secure Score & Security Compliance Toolkit	Technisch, Organisatorisch
M3	C	Microsoft Purview Information Protection	Technisch, Organisatorisch
M4	C, I, A	Datenschutz-Folgenabschätzungen (DSFA)	Organisatorisches
M5	C	Microsoft 365 IAM & Privileged access management	Technisch, Organisatorisch
M6	C	Microsoft Purview Compliance Manager	Technisch, Organisatorisch
M7	C	Data Subject Request	Technisch, Organisatorisch
M8	C, I, A	Microsoft Public Sector Cloud Design Schulung	Organisatorisches
M9	C, I	Microsoft Purview Customer Lockbox	Technisch, Organisatorisch
M10	C, I	Verschlüsselung	Technisch, Organisatorisch
M11	C, I	Microsoft 365 Hybrid mit Exchange und SharePoint	Technisch, Organisatorisch
M12	C, I, A	Vertragswerk	Vertragliche
M13	C, I, A	Shared Responsibility Model	Organisatorisch, Vertraglich
M14	C, I, A	Privacy Management für Microsoft 365	Technisch, Organisatorisch

Tabelle 4 – Liste der Massnahmen

4.1 M1 – ISO 27001

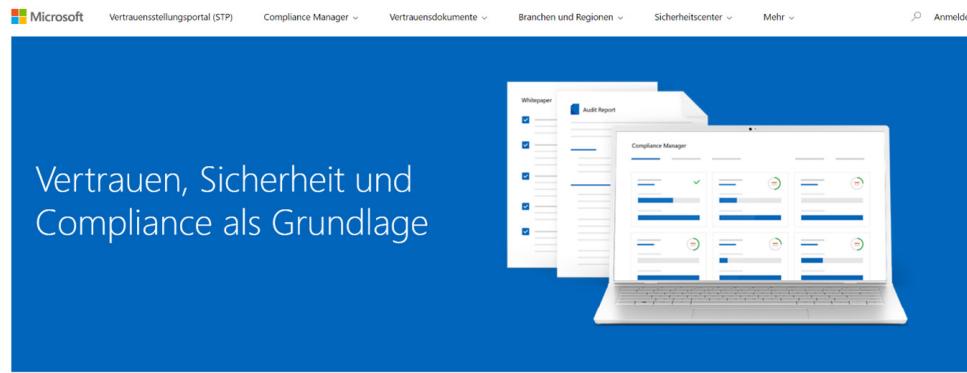
ISO/IEC 27001 ist die internationale Norm zur Implementierung eines Informationssicherheits-Managementsystems (ISMS) und beschreibt Kontrollziele und Massnahmen, die dazu beitragen, die Sicherheit von Informationsbeständen zu gewährleisten.

Ein ISMS beschreibt die notwendigen Methoden und Nachweise im Zusammenhang mit den Anforderungen, die für eine zuverlässiges Verwaltung der Sicherheit von Informationen in jeder Art von Organisation erforderlich sind.

Wichtig ist hierbei, dass Microsoft selbst nach ISO 27001 auditiert und zertifiziert ist. Eine Liste der nach ISO 27001 zertifizierten Cloud-Dienste, einschließlich Microsoft 365 und Office 365, finden sich in der offiziellen Dokumentation¹⁸. Bestandskunden finden die ISO 27001-Auditberichte im Microsoft Trust Center¹⁹.

18 <https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001#microsoft-in-scope-cloud-platforms--services>

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



Prüfungsberichte

Überprüfen Sie die verfügbaren unabhängigen Prüfungsberichte für die Microsoft-Clouddienste, die Informationen bereitstellen zur Einhaltung von Datenschutzstandards und gesetzlicher Bestimmungen, z. B. der Internationalen Organisation für Normung (ISO), des Service Organization Controls (SOC), des National Institute of Standards and Technology (NIST), des Federal Risk and Authorization Management Program (FedRAMP) und der Datenschutz-Grundverordnung (DSGVO).



SOC



FedRAMP



ISO 27001



PCI/DSS

Abbildung 1 – Microsoft Service Trust Portal

Zusätzlich zur Einhaltung der ISO 27001-Norm, bietet Microsoft seinen Kunden eine Liste der wichtigsten Prioritäten für die ersten 30 Tage, 90 Tage und darüber hinaus²⁰ um ihre eigenen ISO/IEC 27001 Anforderungen zu erfüllen. Bitte lesen Sie den Leitfaden zur **Cloud Governance & Security im öffentlichen Sektor der Schweiz**, um alle verfügbaren Optionen besser zu verstehen.

4.2 M2 – MICROSOFT SECURE SCORE & SECURITY COMPLIANCE TOOLKIT

Um die gesetzlichen Anforderungen zu erfüllen, ist ein hohes Mass an grundlegender IT-Sicherheit erforderlich. Der Microsoft Secure Score misst das Sicherheitsniveau des Unternehmens und gibt Hinweise zur Verbesserung auf der Grundlage bewährter Best Practices. Darüber hinaus stellt Microsoft auch das Security Compliance Toolkit für Administratoren zur Verfügung, um die empfohlenen Sicherheitskonfigurationen zu kontrollieren und anzuwenden.

Microsoft Secure Score

Microsoft Secure Score ist ein Werkzeug welches Metriken, Empfehlungen und Anleitungen zur Verbesserung der Sicherheit der Microsoft 365 bezogenen Ressourcen Ihres Unternehmens bietet. Secure Score bewertet den Sicherheitsstatus von Identitäten, Geräten, Informationen, Anwendungen und der Infrastruktur und zeigt die Ergebnisse in einer Punktzahl an. Eine konkrete Liste mit priorisierten Verbesserungsmassnahmen liefert Details darüber, warum und wie diese verbessert werden sollten.

Das Microsoft Secure Score Dashboard ist der zentrale Ort, mit dem Unternehmen die Sicherheitskonfigurationen in ihrem Tenant anhand der aktuellsten «Best Practices» kontrollieren und verwalten können. Die Verbesserungsmassnahmen werden regelmässig überprüft, so dass die Kunden rechtzeitig informiert werden, wenn eine Konfiguration nicht mehr den Anforderungen entspricht. Dies kann das Ergebnis einer Konfigurationsänderung oder einer aktualisierten «Best Practice» sein. Der Secure Score ermöglicht es den Behörden Risiken entsprechend ihrer Risikobereitschaft gezielt zu mitigieren oder zu akzeptieren und dokumentieren.

20 <https://docs.microsoft.com/en-us/compliance/regulatory/iso-action-plan>

Der Secure Score wird beeinflusst durch:

- Wie die empfohlenen Sicherheitsmassnahmen konfiguriert werden
- Wie sicherheitsrelevante Aufgaben durchgeführt werden
- Ob Verbesserungsmassnahmen durch alternative Lösungen von Drittanbietern durchgeführt wurden

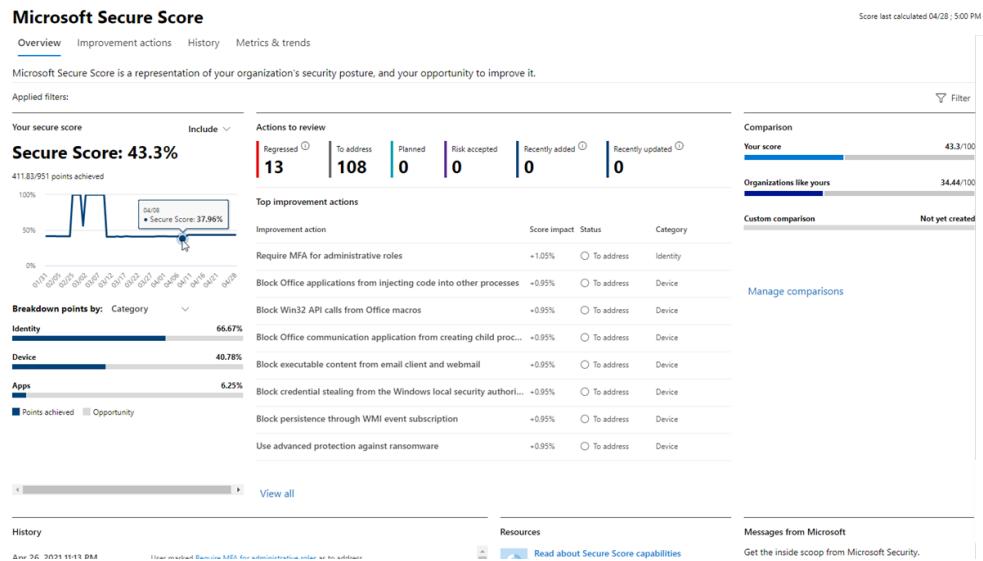


Abbildung 2 – Microsoft Secure Score

Security Compliance Toolkit

Das Security Compliance Toolkit (SCT) ist ein Werkzeug, mit dem IT-Sicherheitsadministratoren die von Microsoft empfohlenen Konfigurationsgrundlagen implementieren können.

SCT erleichtert den IT-Administratoren die Verwaltung der Active Directory Group Policies (GPOs) des Unternehmens. Bestehende GPOs können mit den von Microsoft empfohlenen Richtlinien verglichen werden und anschliessend über Active Directory, Microsoft MDM-Richtlinien oder individuell lokale Richtlinien angewendet werden.

Die folgenden Richtlinien sind verfügbar:

- Windows 10 security baselines
- Windows Server security baselines
- Microsoft Office security baseline
- Microsoft Edge security baseline

4.3 M3 – MICROSOFT PURVIEW INFORMATION PROTECTION

Microsoft Purview Information Protection unterstützt Unternehmen bei der Klassifizierung, Kennzeichnung und dem Schutz von Daten auf der Grundlage ihrer Sensibilität.

Organisationen verwenden sogenannte Labels als Unterstützung folgender Aktivitäten:

- Die Benutzer verstehen die Bedeutung der Informationen die sie verarbeiten
- Compliance Beauftragte kennen die Speicherorte sensibler Informationen
- Sicherheitsadministratoren setzen Richtlinien für den Datenzugriff und den Schutz vor Datenverlusten (DLP) auf der Grundlage der Labels um

Microsoft Purview Information Protection (MIP) ist ein Framework, das mehrere technische Lösungen umfasst, um ein effektives Klassifizierungssystem zum Schutz sensibler Daten in Ihrem Unternehmen zu unterhalten. MIP bietet einheitliche Funktionen, um Daten zu identifizieren, zu schützen und Datenverluste in allen Microsoft 365 Anwendungen (z. B. Word, PowerPoint, Excel, Outlook) und Diensten (z. B. Teams, SharePoint und Exchange) zu verhindern.

Azure Information Protection (AIP) ist eine der Komponenten von MIP. AIP wird für die Klassifizierung von Informationen durch Labels verwendet. Mit AIP als Grundlage, können Organisationen den Zugriff und die Nutzung von Informationen innerhalb und außerhalb der Unternehmung kontrollieren.

Die Bestandteile von Microsoft Purview Information Protection helfen bei der Einhaltung von Vorschriften, bei denen Daten je nach ihrer Klassifizierung, unterschiedlich behandelt werden müssen.



Abbildung 3 – Microsoft Purview Information Protection

Durch die Kombination mit Conditional Access²¹ bietet MIP zusätzliche Möglichkeiten:

- Blockieren des Zugangs zu sensiblen Inhalten, wenn die Wahrscheinlichkeit einer riskanten Anmeldung besteht (d.h. der Anmeldeversuch wurde nicht vom rechtmäßigen Inhaber eines Benutzerkontos durchgeführt).
- Anfordern einer Anmeldung mit mehreren Faktoren, um geschützte Dokumente zu öffnen.
- Beim Zugriff auf sensible Informationen müssen die Geräte mit den Unternehmensrichtlinien übereinstimmen, z.B. die Mindestversion eines Betriebssystems erfüllen, Teil der Domäne sein oder spezifische PIN- bzw. Kennwortrichtlinien erfüllen.

4.4 M4 – DATENSCHUTZ-FOLGENABSCHÄTZUNGEN (DSFA)

In bestimmten Situationen verlangt die Datenschutzgesetzgebung die Durchführung einer Datenschutz-Folgenabschätzung (DSFA), um Daten zu verarbeiten, die «voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge» hat (Beispiel aus DSGVO Art. 35, Abs. 1). Ob eine Datenschutz-Folgenabschätzung erforderlich ist, hängt davon ab, wie eine Organisation Microsoft 365 nutzt und welche Arten von personenbezogenen Daten verarbeitet werden.

Die Erstellung einer Datenschutz-Folgenabschätzung (Englisch: Data Protection Impact Assessment, DPIA) kann zeitaufwändig sein. Obwohl die DPIA jedes Kunden aufgrund der spezifischen Nutzung und Konfiguration von Microsoft 365 unterschiedlich ausfällt, kann die anpassbare DPIA-Vorlage²² Zeit sparen.

²¹ <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

²² <https://www.microsoft.com/en-us/download/details.aspx?id=102398>

Contents

Introduction	1
1. DPIA setup and changelog	4
2. About the processing activity in scope	7
3. Data necessity, proportionality and transparency	11
3.1 Lawfulness, Fairness and Transparency.....	11
3.2 Purpose Limitation	12
3.3 Data Accuracy and Data Minimization	13
3.4 Accountability	13
3.5 Data Subject Rights	15
4. Data Security	16
5. Data Processors and International Transfers	19
6. Stakeholder engagement	22
7. Diagram of Personal Data Flows	24
8. Data Protection Risk Identification, Assessment and Mitigation.....	25

Abbildung 4 – Vorlage für Datenschutz-Folgenabschätzungen (DPIA)

Weitere Informationen für eine Microsoft 365 spezifische DPIA finden Kunden in der offiziellen Dokumentation²³.

4.5 M5 – MICROSOFT 365 IAM & PRIVILEGED ACCESS MANAGEMENT

Ständiger Zugriff bestimmter Benutzer auf sensible Daten in den Microsoft 365 Online-Services ist ein potenzielles Risiko für kompromittierte Konten oder Bedrohungen von innen, auch als «insider-risk» bezeichnet. Eine aktive Verwaltung von privilegierten Zugriffen schützt Ihr Unternehmen vor Sicherheitsverletzungen und hilft bei der Einhaltung von «Best Practices», indem der ständige Zugriff auf sensible Daten oder der Zugriff auf kritische Konfigurationseinstellungen eingeschränkt wird.

Anstelle des ständigen Zugriffs von Administratoren, werden zeitlich begrenzte Zugriffsregeln für Aufgaben implementiert, die erhöhte Berechtigungen erfordern. Durch die Aktivierung von «Privileged Access Management (PAM)» in Microsoft 365, kann Ihre Organisation ohne ständige Zugriffsrechte arbeiten und bietet eine Abwehr gegen daraus entstehende Schwachstellen. «Privileged Access Management» erfordert, dass Benutzer einen «Just-in-Time»-Zugriff für die zeitlich begrenzte Ausführung von kritischen Aufgaben über einen Genehmigungsprozess beantragen.

Darüber hinaus gibt es verschiedene Mechanismen, um das Nutzerverhalten zu analysieren und festzustellen, wann ein Nutzer aufgrund früherer Aktivitäten gefährdet ist (z.B. beim gleichzeitigen Zugriff auf Dienste von zwei voneinander weit entfernten Standorten). Diese Mechanismen sind Teil der so genannten «Identity Protection», welche die Organisation dabei unterstützt verdächtiges Nutzer- und Anmeldeverhalten zu erkennen, den unerwünschten Zugriff auf Daten zu verhindern und Zugriffe, von welchen ein hohes Risiko ausgeht, zu untersuchen. Damit kann «Identity Protection» zur Einhaltung bestimmter Vorschriften beitragen.

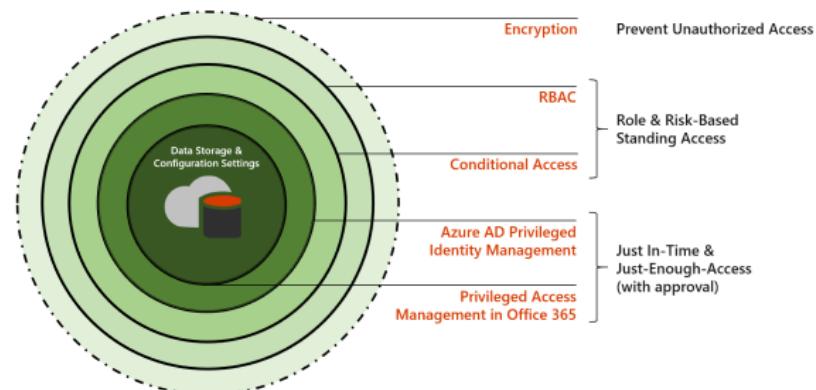


Abbildung 5 – Privileged Access Management für Microsoft 365

23 <https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365>

4.6 M6 – MICROSOFT PURVIEW COMPLIANCE MANAGER

Der Microsoft Purview Compliance Manager hilft bei der Einhaltung von Vorschriften, indem er Massnahmen empfiehlt, um die jeweils geltenden Branchenvorschriften und Standards einzuhalten, wie z.B. Datenschutzbestimmungen. Zusätzlich bietet der Compliance Manager folgende Funktionen:

- Zuweisung von Compliance-Aktivitäten und deren Verfolgung und Aufzeichnung
- Bewertung und Priorisierung von Kontrollzielen
- Sicherer Aufbewahrungsort für Dokumentation und andere Bestandteile
- Erzeugt detaillierte Berichte, die Wirtschaftsprüfern, Aufsichtsbehörden oder anderen Beteiligten zur Verfügung gestellt werden können

Mit vorgefertigten «Assessments», detaillierten Schritt-für-Schritt-Anleitungen zu vorgeschlagenen Verbesserungsmassnahmen und einer risikobasierten Compliance-Bewertung, hilft der Compliance Manager die Compliance-Situation zu erkennen, laufend zu verbessern und den Fortschritt kontinuierlich zu messen.

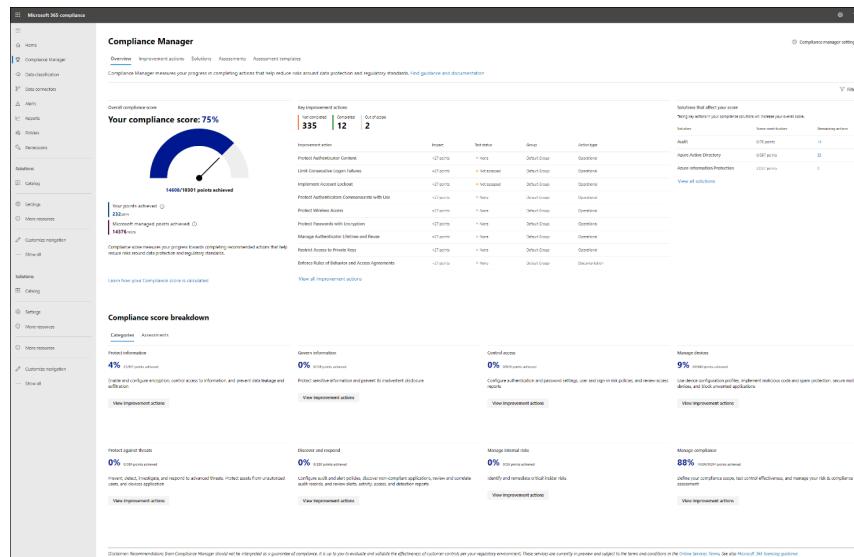


Abbildung 6 – Microsoft 365 Purview Compliance Manager

Für Unternehmen, die eine Vielzahl von Vorschriften einhalten müssen, ist es oft schwer einen Einstieg zu finden. Der Microsoft Purview Compliance Manager bietet einen umfassenden Satz an Vorlagen zur Bewertung dieser Vorschriften. Diese Vorlagen helfen Unternehmen bei der Einhaltung nationaler, regionaler und branchenspezifischer Anforderungen an die Erfassung und Verwendung von Daten. Mit dem Compliance Manager kann festgestellt werden, inwieweit die bestehenden Vorschriften mit bestimmten gesetzlichen Anforderungen übereinstimmen.

Neue Vorlagen werden dem Compliance Manager hinzugefügt, wenn neue Gesetze und Vorschriften in Kraft treten. Die Compliance Manager Vorlagen werden auch dann aktualisiert, wenn sich die zugrundeliegenden Gesetze oder Vorschriften ändern, und unterstützt so bei folgenden Aktivitäten:

- Integrierte Bewertungen für Branchenvorschriften und Standards
- Benutzerdefinierte Bewertungen zur Erfüllung der individuellen Compliance-Anforderungen
- Workflow-Funktionen, die die Organisation bei der Durchführung von Risikobewertungen unterstützen
- Detaillierte Schritt-für-Schritt-Anleitungen für Verbesserungsmassnahmen
- Risikobasierte Bewertung der Einhaltung von Vorschriften

Eine vollständige Liste der Bewertungsvorlagen²⁴ finden Kunden in der offiziellen Dokumentation.

Durch die Nutzung von Cloud Services entstehen gemeinsame Verantwortlichkeiten zwischen der Behörde und dem Cloud Anbieter im Sinne des «Shared Responsibility Model» (siehe Kapitel 4.13). Der Compliance Manager hilft zu klären, welche Kontrollziele von Microsoft verwaltet werden und welche in der Verantwortung des Kunden liegen.

²⁴ <https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-list?view=o365-worldwide#overview>

4.7 M7 – DATA SUBJECT REQUEST

Bestimmte Datenschutzgesetze gewähren natürlichen Personen (Data Subject), die über eine Kennung (z.B. Name, ID-Nummer usw.) identifiziert werden können, Rechte in Bezug auf ihre personenbezogenen Daten, wie z.B. die Anforderung von Kopien personenbezogener Daten, deren Berichtigungen, die Einschränkung der Verarbeitung, die Löschung von Daten oder den Erhalt der personenbezogenen Daten in elektronischem Format. Ein formaler Antrag zur Ergreifung von Massnahmen in Bezug auf personenbezogenen Daten wird als Data Subject Request (DSR) bezeichnet. Microsoft 365 bietet integrierte Tools zur Erfüllung eines DSR.

Der erste Schritt bei der Beantwortung einer DSR ist die Identifizierung der personenbezogenen Daten, die Gegenstand der Anfrage sind. Dies geschieht durch die Suche nach den angeforderten personenbezogenen Daten mithilfe der «Subject Rights Requests»-Funktionen in Microsoft 365.

Neben der Reaktion auf einen DSR mit den integrierten Microsoft 365 Tools, bietet Microsoft Priva²⁵ zusätzliche Funktionen zur Untersuchung und Bearbeitung eines DSR, wie z.B. die Identifizierung kritischer Datenschutzrisiken und Konflikte, die Automatisierung von Datenschutzhängen, sowie die Befähigung von Mitarbeitenden, intelligente Entscheidungen im Umgang mit personenbezogenen Daten zu treffen.

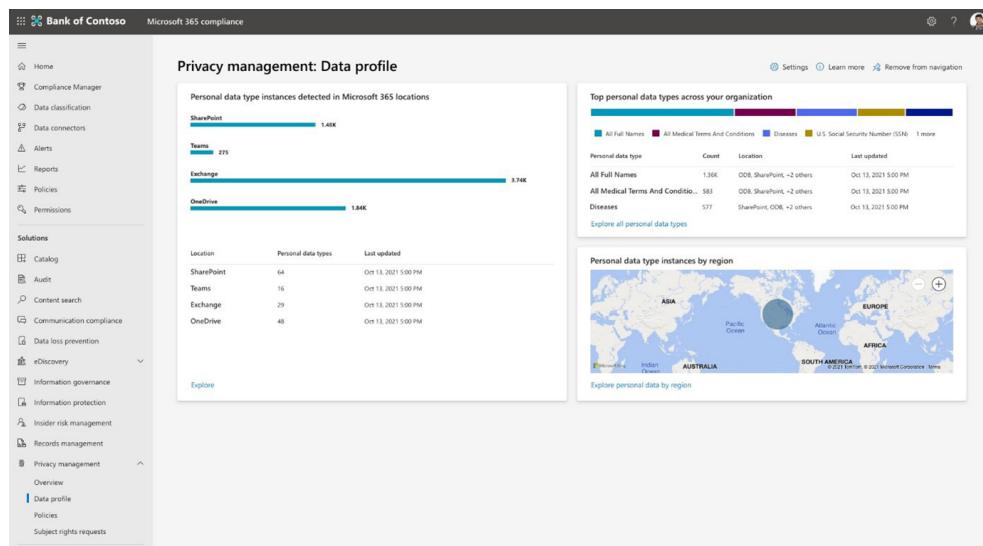


Abbildung 7 – Microsoft 365 Priva Dashboard

4.8 M8 – MICROSOFT PUBLIC SECTOR CLOUD DESIGN SCHULUNG

Als Grundlage für die effektive Nutzung von Microsoft 365 als Cloud-Plattform, einschließlich der in diesem Leitfaden vorgestellten Komponenten und Konzepte, müssen Schulungsmassnahmen für alle involvierten Mitarbeitenden durchgeführt werden.

Unabhängig von der Rolle im Unternehmen (z.B. CISO oder IT-Administrator), bietet eine Schulung zum Microsoft Public Sector Cloud Design die Möglichkeit die Einführung von Cloud-Diensten voranzutreiben und gleichzeitig die Einhaltung von Vorschriften zu unterstützen.

Neben der Vertiefung Ihrer Kenntnisse zu den Funktionen von Microsoft 365, macht eine spezialisierte Schulung deutlich, was die Einführung eines «Software-as-a-Service» Modells für Behörden bedeuten.



Abbildung 8 – Struktur der Microsoft 365 Public Sector Cloud Design Schulung

25 <https://www.microsoft.com/en-ww/security/business/privacy/privacy-management-software>

Einige Microsoft-Partner bieten eine Einführung in das Microsoft Public Cloud Design für den öffentlichen Sektor an, sowie zusätzliche Schulungen zu den rechtlichen Grundlagen, den spezifischen technologischen Möglichkeiten des Microsoft 365 Ökosystems und dem angestrebten Betriebsmodell. Hierbei handelt es sich primär um technische Unterstützung, welche eine allenfalls notwendige rechtliche Überprüfung nicht ersetzt.

Basis	Technology	Betrieb
<ul style="list-style-type: none"> – Einführung Cloud Design – Datenschutzgesetz (revDSG) – Informationsschutzverordnung (ISchV) – Information Security (ISO 27001) – Informationsklassifizierung 	<ul style="list-style-type: none"> – Microsoft Purview Information Protection – Microsoft Purview Compliance Manager – Microsoft 365 Hybrid deployments – Privacy Management for Microsoft 365 	<ul style="list-style-type: none"> – Blueprint-Bereitstellung – Konformitätsanalyse – Richtlinien erstellen – Umgebung einrichten – Kontinuierliche Überprüfung – Überwachung

Abbildung 9 – Microsoft Public Sector Cloud Design Schulung

This measure supports the following targets:

- Preventing incorrect manipulation
- Ensuring operational continuity
- Increase IT departments' understanding of the technologies, risks, and opportunities.

4.9 M9 – MICROSOFT PURVIEW CUSTOMER LOCKBOX

Für jeden Microsoft 365 Service können autorisierte Administratoren das Microsoft 365 Admin Center nutzen, um online Support-Anfragen zur Behebung von Problemen zu stellen. Das Support-Team von Microsoft 365 behebt diese Probleme nur auf Anfrage des Kunden und nur so lange das Support-Ticket offen ist.

Fast alle Fehlerbehebungen in Microsoft 365 sind automatisiert und erfordern keinen Zugriff auf Kundendaten. Sollte jedoch ein Zugriff auf die Cloud-Umgebung oder die Daten des Unternehmens erforderlich sein, muss jeder Microsoft-Mitarbeitende ein robustes Verfahren durchlaufen, um die Genehmigung für den Zugriff während eines Supportfalls zu erhalten.

Die zusätzliche Customer Lockbox Funktion für Microsoft 365 ermöglicht es Organisationen, die Anfragen von Microsoft für den Zugriff auf Ihre Cloud-Umgebung oder Daten zu überprüfen und zu genehmigen/ abzulehnen. So kann z.B. beurteilt werden, ob Informationen, die während einer Supportanfrage weitergegeben werden müssen, vertraulich sind und ob diese eingesehen werden dürfen oder nicht.

Der Zugang wird nur für ein kurzes Zeitfenster gewährt. Anschliessend wird er unabhängig davon, ob das Problem gelöst wurde oder nicht, wieder automatisch entzogen.

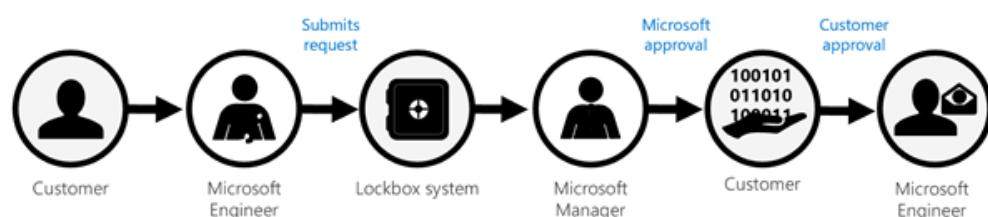


Abbildung 10 – Customer Lockbox Prozess

Darüber hinaus werden Customer Lockbox-Anfragen in einem Audit-Protokoll gespeichert. So lässt sich nachvollziehen, wann diese Art von Anfrage gestellt wurde, und ob sie angenommen oder abgelehnt wurde. Über die Suche für Audit-Protokolle im Security & Compliance Center können diese Protokolle bei Bedarf abgerufen werden.

Diese Massnahme unterstützt die folgenden Zielsetzungen:

- Wahrung der Vertraulichkeit von Kundendaten

4.10 M10 – VERSCHLÜSSELUNG

Verschlüsselung ist ein wichtiger Bestandteil der Strategie zum Schutz von Dateien und Informationen. Unternehmen erstellen, teilen und speichern sensible Daten vor Ort, in der Cloud oder in mehreren Clouds. Aufgrund der Geschäftstätigkeiten und zur Einhaltung gesetzlicher Vorschriften, sollten sensible Daten sicher gespeichert und verschlüsselt werden. Microsoft 365 bietet Lösungen für die Verschlüsselung von Datenträgern, Dateien, Datenbanken und Postfächern in Office 365, sowohl im Ruhezustand als auch bei der Übertragung.

Aufgrund unterschiedlicher Geschäftsanforderungen und Regulierung, stehen Unternehmen verschiedene Verfahren zur Verschlüsselung der Daten in der Microsoft Cloud-Plattform zur Verfügung.

Mit Microsoft 365 können mehrere Ebenen und Typen der Verschlüsselung kombiniert werden, um Ihre Daten zu schützen. So können beispielsweise E-Mail-Nachrichten selbst, als auch die Kommunikationskanäle, über die Ihre E-Mails laufen, verschlüsselt werden. Daten werden sowohl im Ruhezustand und bei der Übertragung verschlüsselt, wobei mehrere starke Verschlüsselungsprotokolle wie TLS/SSL, IPSec und Advanced Encryption Standard (AES) verwendet werden.

Gemäss den Richtlinien des «Shared Responsibility Models» (siehe Kapitel 4.13) sind letztlich die CISOs und Datenverantwortliche von Unternehmen dafür verantwortlich, das richtige Verschlüsselungsverfahren zum Schutz der Daten auszuwählen und zu implementieren.

Wenn eine Organisation eine der folgenden Anforderungen erfüllt, kann es sinnvoll sein, eine Kombination verschiedener Verschlüsselungstypen und Technologien, wie z. B. Microsoft Purview Information Protection (MIP) (siehe Kapitel 4.3) zu verwenden, um sensible oder hochsensible Informationen zu schützen:

- Nur autorisierte Personen sollen in der Lage sein, hochsensible Inhalte zu entschlüsseln
- Microsoft darf keinen Zugang zu hochsensiblen Daten haben
- Wenn die Schlüssel innerhalb einer geografischen Grenze und unter Ihrer eigenen Kontrolle bleiben müssen

Eine typische Datenlandschaft einer Organisation



Abbildung 11 – Typische Datenlandschaft einer Organisation

Hierfür bietet Microsoft die folgenden Verschlüsselungslösungen an:

- Microsoft Managed Key (MMK)
- Bring Your Own Key (BYOK)
- Double Key Encryption (DKE)

Diese Verschlüsselungslösungen können bei Problemen im Zusammenhang mit der Übermittlung in Drittländer, ausländischen Rechtsvorschriften, der Offenlegung von Daten, oder bei strafrechtlichen Ermittlungen helfen.

Ebenfalls können die Verschlüsselungsschlüssel in spezieller Hardware (HSM) gespeichert werden, auf die Microsoft keinen Zugriff hat. Dadurch können die Schlüssel zusätzlich auch außerhalb des Cloud-Dienstes selbst gespeichert werden, zum Beispiel im Double Key Encryption (DKE) Verfahren. DKE kann für den Umgang mit extrem sensiblen Daten nützlich sein.

Je nach Verschlüsselungsoption kann die Funktionalität einiger Microsoft Dienste eingeschränkt sein (z.B. Indexierung von Dokumenten oder Malwareanalyse). Vor der Entscheidung für eine bestimmte Art der Verschlüsselung, sollte stets eine Folgenabschätzung durchgeführt werden.

Einen vollständigen Vergleich²⁶ der verschiedenen Verschlüsselungstypen finden Sie auf dem offiziellen Microsoft-Blog.

4.11 M11 – MICROSOFT 365 HYBRID MIT EXCHANGE UND SHAREPOINT

Eine hybride Bereitstellung bietet Unternehmen ein durchgängiges Benutzererlebnis und eine ganzheitliche Administration der lokalen Dienste und der Cloud. Darüber hinaus kann eine hybride Bereitstellung als Zwischenschritt zum vollständigen Umstieg auf Office 365 dienen.

Mit einer hybriden Umgebung für Exchange und SharePoint, können Daten, die nicht in der Cloud abgelegt werden sollen, lokal gespeichert werden und bietet dennoch ein nahtloses Benutzererlebnis.

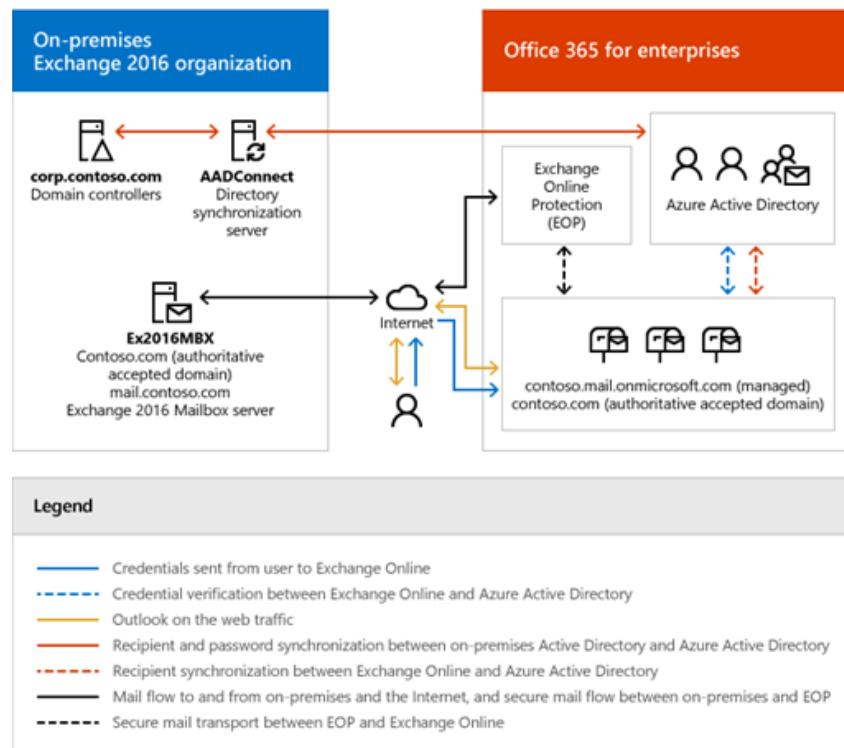


Abbildung 12 – Microsoft 365 Hybrid-Konfiguration für Exchange

²⁶ <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/understanding-microsoft-information-protection-encryption-key/ba-p/2214589>

Mithilfe von Regeln zur Klassifizierung und Data Loss Prevention (DLP) kann verhindert werden, dass bestimmte Informationen in der Cloud gespeichert werden. Stattdessen werden die Benutzer angewiesen, diese Informationen in einer lokalen SharePoint-Umgebung zu speichern.

4.12 M12 – 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:

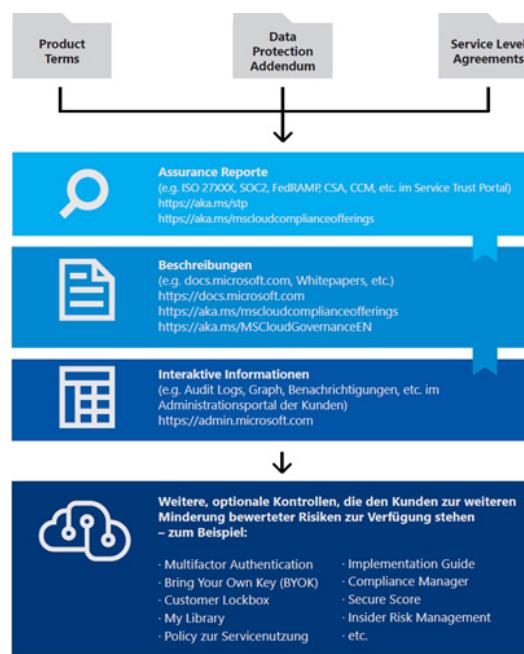


Abbildung 13 – Microsoft Assurance Framework

- 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**, 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.

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:

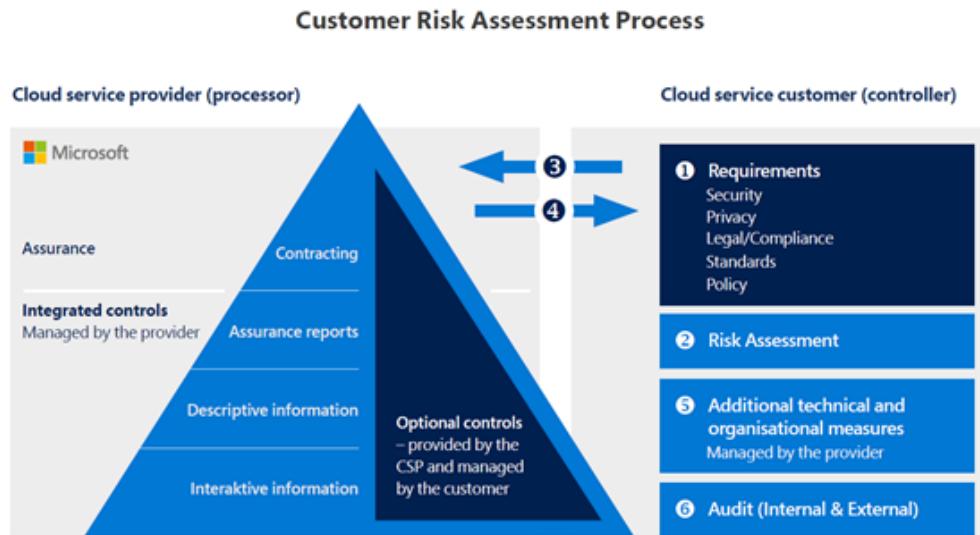


Abbildung 14 – Customer Risk Assessment Prozess

Diese Massnahme unterstützt die folgenden Zielsetzungen:

- Sicherstellung der Compliance
- Einschränkungen von Risiken durch Richtlinien

4.13 M13 – 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 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.



Abbildung 15 – Shared Responsibility Model

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 Microsoft 365 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 Portal²⁷ abrufbar sind.

Diese Massnahme unterstützt die folgenden Zielsetzungen:

- Verantwortlichkeiten zwischen Provider und Kunde regeln
- Unterstützung der Risikoeinschätzung

4.14 M14 – PRIVACY MANAGEMENT FÜR MICROSOFT 365

Die exponentielle Zunahme von «Hybrid»- und «Remotework» hat dazu geführt, dass Mitarbeitende flüssig zwischen beruflichen und privaten Aktivitäten wechseln. Infolgedessen werden personenbezogene Daten immer «mobiler» und über eine Vielzahl von Geräten und Clouds abgerufen, was die Daten anfällig für komplexe Angriffe macht. Dadurch wächst die Sorge um das Vertrauen in Technologien und Organisationen, die persönlichen Daten verarbeiten. Gesetzgeber reagieren auf diese Bedenken, indem sie Vorschriften zum Schutz personenbezogener Daten erlassen und den Verbrauchern das Recht auf ihre Daten einräumen, so dass Unternehmen gezwungen sind, den Datenschutz zu einem zentralen Bestandteil ihrer Geschäftstätigkeit zu machen.

Um auf diese Herausforderungen reagieren zu können, ermöglicht «Privacy Management» für Microsoft 365 die automatische und kontinuierliche Identifikation von personenbezogenen Daten in der Microsoft 365 Umgebung des Kunden, indem es Datenklassifizierung und andere Benutzerinformationen nutzt. Im Ergebnis erhalten Unternehmen einen Gesamtüberblick über ihre Datenschutzsituation, einschliesslich der Mengen, der Kategorie, des Standorts und der Bewegung von personenbezogenen Daten innerhalb der Microsoft 365 Umgebungen.

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

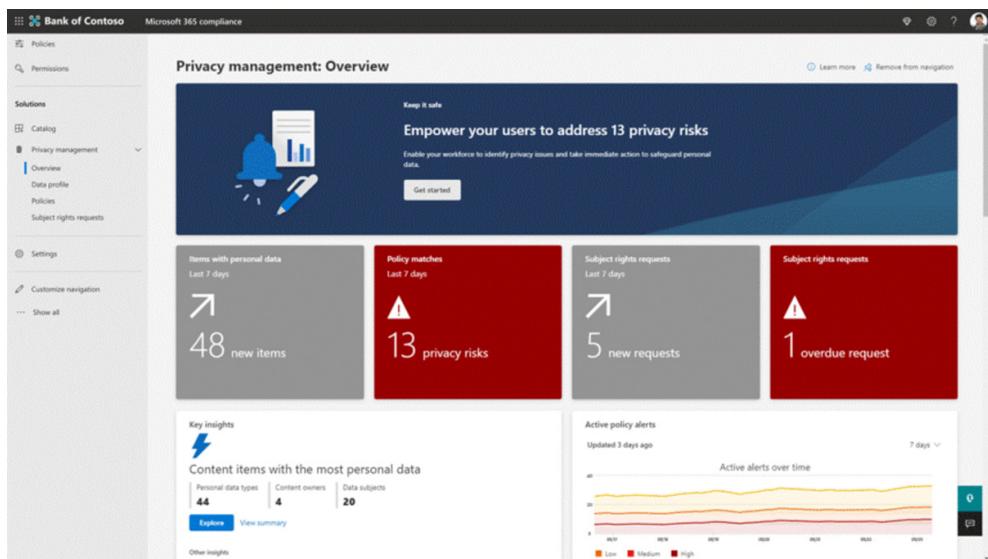


Abbildung 16 – Dashboard zur Datenschutzverwaltung für Microsoft 365

Privacy Management für Microsoft 365 ermöglicht Unternehmen:

- Identifizierung kritischer Datenschutzrisiken und Konflikte
- Automatisierung von Datenschutzmassnahmen und Beantwortung von Anfragen der Betroffenen
- Befähigung der Mitarbeitenden, fundierte Entscheidungen im Umgang mit Daten zu treffen



APPENDIX : WICHTIGE VERTRAGS GRUNDLAGEN UND LINKS

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

Dokument oder Themenbereich	Verweise
Microsoft-Datenschutzbestimmungen	https://privacy.microsoft.com/de-de/privacystatement
Datenschutznachtrag zu den Produkten und Services von Microsoft (DPA)	https://aka.ms/dpa
Universelle Lizenzbedingungen für Onlinedienste	https://www.microsoft.com/licensing/terms/product/ForOnlineServices
Microsoft Business and Services Agreement (MBSA) oder Microsoft-Kundenvereinbarung oder andere Programme je nach Umständen	MBSA: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4f5aA Kundenvereinbarung: https://www.microsoft.com/licensing/docs/customeragreement
Technische Dokumentation der Microsoft 365 Dienste	https://docs.microsoft.com/de-ch/
Microsoft Trust Center (Compliance- und Sicherheitsdokumentation)	https://www.microsoft.com/de-ch/trust-center
SLA-Dokumentation für alle Microsoft Online-Dienste	https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

Tabelle 5 – Zusammenstellung wichtiger Informationsquellen



Danke
Merci
Grazie
Engraziel