

# MICROSOFT

## Whitepaper Cloud und Behörden



## 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.

# Inhalt

<b>I. CLOUD UND BEHÖRDEN IN DER SCHWEIZ.....</b>	<b>5</b>	<b>III. HÄUFIGE FRAGEN UND ANTWORTEN .....</b>	<b>14</b>
A. EINFÜHRUNG.....	5	1. Datenherrschaft; gibt es eine klare Definition und Vereinbarung bezüglich der Herrschaft des Kunden über seine Daten?.....	14
B. CLOUD ALS CHANCE FÜR DIE DIGITALISIERUNG .....	6	2. Datenstandort; ist jederzeit klar, wo die Daten des Kunden gespeichert sind und wo sich die Rechenzentren befinden?.....	14
a. Erhöhte Sicherheit .....	6	3. Wie werden Änderungen an der Sicherheits-, Datenschutz- und Compliance-Dokumentation, den Listen der Unterauftragnehmer, den Allgemeinen Geschäftsbedingungen usw. gehandhabt? .....	18
b. Compliance-Verbesserungen .....	6	4. Hat der Kunde die Möglichkeit, Prüfungen selber durchzuführen oder durch eine unabhängige, akkreditierte und vom Kunden ausgewählte Prüfgesellschaft durchführen zu lassen? .....	18
c. Höhere Zuverlässigkeit und Ausfallsicherheit .....	6	5. Wie werden die Audit-Logs gesichert? - Wie und wie oft werden sie zum Schutz vor unentdeckten Sicherheitsvorfällen überprüft? .....	18
C. HERAUSFORDERUNGEN .....	6	6. Ist Microsoft eindeutig zur Einhaltung von Datenschutzgesetzen und -verordnungen verpflichtet?.....	18
1. Kontrolle von Daten als Kernthema .....	7	7. Erfüllt die Datenbearbeitungsvereinbarung die gesetzlichen Mindestanforderungen? .....	18
2. Das Shared Responsibility Modell.....	7	8. Kann Microsoft die «Exit-Strategie» eines Kunden unterstützen? - Wie? .....	18
3. Ausübung von Kontrolle in der Cloud.....	8	9. Gibt es Dokumentation darüber, wie die Onlinedienste betrieben, gesichert und gewartet werden? .....	19
<b>II. RECHTLICHE HERAUSFORDERUNGEN .....</b>	<b>9</b>	10. Inwieweit werden internationale Sicherheits- und Datenschutz-Standards unterstützt? .....	19
A. ÜBERSICHT.....	9	11. Wie wird die geografische Resilienz sichergestellt? .....	20
1. Einleitung .....	9	12. Wie wird die Datenaufbewahrung gehandhabt? .....	20
2. Cloud Computing als eigener Auslagerungssachverhalt.....	9	13. Werden Penetrationstests sowohl für Netzwerke als auch für Anwendungen durchgeführt? .....	20
3. Ausland.....	9	14. Wie wird sichergestellt, dass der Kunde seine Daten im Falle von Fehlern oder Verlusten wiederherstellen kann? .....	21
B. DATENSCHUTZRECHTLICHE REGELUNGEN IN BUND UND KANTONEN.....	9	15. In welchem Umfang wird Verschlüsselung verwendet in Bezug auf ruhende Daten («at rest») und für Daten «in transit»?.....	22
1. Allgemeines.....	9	16. Hat der Kunde Zugriff auf zusätzliche Verschlüsselungstechnologien inkl. BYOK etc.? .....	23
2. Datenbearbeitung durch Dritte im Auftrag .....	9	a. Bring-Your-Own-Key/Hold-Your-Own-Key (BYOK/HYOK) .....	23
3. Die gängigsten Vorgaben im Einzelnen.....	10	17. Welche Sicherheits- und Datenschutzprüfungen unternimmt Microsoft in Bezug auf eigene Mitarbeiter und die Mitarbeiter von Subunternehmen? .....	24
a. Vertragliche Vereinbarung.....	10	18. Wie handelt Microsoft das Identitäts- und Zugriffsmanagement? .....	24
b. Bearbeitung nach Weisung und im Interesse des öffentlichen Organs .....	10	19. Wie geht Microsoft mit der Separierung von Kundendaten in einer Multi-Tenant-Umgebung um? .....	24
c. Einbezug weiterer Datenbearbeiter .....	10	20. Wie werden Anfragen von Behörden nach Datenzugriff oder Datenherausgabe behandelt? .....	25
d. Datensicherheit .....	11	21. Werden Subunternehmer eingesetzt? Und wenn ja, unter welchen Bedingungen und wofür? .....	27
e. Auslandsbezüge.....	12		
4. Geheimhaltungsvorschriften.....	13		
5. Kritische Daten.....	13		

22. In welchem Umfang werden Daten in Länder ausserhalb der EU/EWR übertragen?	
Welche rechtlichen Kontrollen, Sicherheits- und Datenschutzmassnahmen stehen dem Kunden zur Verfügung, um eine Risikobewertung durchzuführen und Übertragungen zu dokumentieren? .....	28
23. Gibt es Hilfestellungen für die Beschaffung, Bereitstellung, Migration und zur Sicherstellung der Compliance von Onlinediensten? .....	28
a. Use Cases von bestehenden Kunden.....	28
b. Cloud-Kostenanalyse (TCO):.....	28
c. Compliance Aufgaben.....	28
d. Optimierung der Cloud-Implementierung .....	29
e. Überwachung und Optimierung von Sicherheit und Compliance .....	29
f. Regulatorische Compliance .....	29
g. Sicherstellung einer optimalen Implementierung und Konfiguration .....	30
h. Leitfaden zur Cloud-Anwendung .....	30
i. Insider-Risikomanagement.....	31
<b>IV. ANHANG – DATENSCHUTZRECHTLICHE BESTIMMUNGEN BUND UND KANTONE .....</b>	<b>32</b>



# I. CLOUD UND BEHÖRDEN IN DER SCHWEIZ

## A. EINFÜHRUNG

Das Thema Cloud-Nutzung durch Behörden ist **hochaktuell**: Der Bundesrat (Regierung) hat im Dezember 2020 einerseits die Cloud-Strategie der Bundesverwaltung verabschiedet und andererseits einen Bericht zur Bedarfsabklärung für eine «Swiss Cloud» zur Kenntnis genommen.

Die **Cloud-Strategie der Bundesverwaltung** sieht unter dem Titel «Cloud-Vision» vor, dass die Bundesverwaltung bis spätestens 2025 über die umfassende Fähigkeit verfügt, IT-Dienste für die Bundesverwaltung kombiniert aus Private Clouds der eigenen Leistungserbringer sowie aus Public Clouds zur Verfügung zu stellen. Dabei wird die Public Cloud explizit als neue strategische IT-Sourcing-Option behandelt (Cloud-Strategie 2020, S. 7 ff.). Die Cloud-Strategie hält in Form eines Grundsatzes (Grundsatz D-1: Datenverarbeitung in Public Clouds schrittweise angehen) fest, dass selbst dann, wenn der rechtliche Rahmen mehr zulässt, in einem ersten Schritt maximal als intern klassifizierte Informationen in einer Public Cloud bearbeitet werden sollen. Für höher klassifizierte Informationen oder besonders schützenswerte Personendaten gelten strengere Vorgaben (Cloud-Strategie, S. 13). Auf den letzten Seiten der Cloud-Strategie der Bundesverwaltung findet sich eine **Roadmap mit Meilensteinen**. Nennenswert sind insbesondere der für das dritte Quartal 2021 vorgesehene Meilenstein «Rahmenverträge für Public Clouds» sowie die Aktualisierung der Cloud-Strategie per Ende 2021. Sodann soll die Bundesverwaltung im ersten Quartal 2022 zur geordneten, sicheren und effizienten Nutzung von IT-Diensten aus der Public Cloud unter Beachtung der Cloud-Prinzipien befähigt sein. Auch wenn die Cloud-Strategie auf die Bundesverwaltung fokussiert, ist davon auszugehen, dass viele Kantone beobachten, wie sich die Situation auf Bundesebene entwickelt und sich in eine ähnliche Richtung bewegen.

Anders als die Cloud-Strategie der Bundesverwaltung bezieht der auf einer Umfrage basierende **Bericht zur Bedarfsabklärung für eine «Swiss Cloud»** explizit auch die Kantone mit ein (siehe Management-Summary auf Seite 4 des Berichts). Die Haupterkenntnis des Berichts besteht darin, dass kein Bedarf für eine «Swiss Cloud» in Gestalt einer öffentlich-rechtlichen Infrastruktur besteht (Bericht Bedarfsabklärung, S. 28). Gefordert wird hingegen eine «Swiss Cloud» als Label in Form geeigneter Rahmenbedingungen und Leitlinien für eine kompetente und sichere Nutzung von Cloud-Leistungen. Der Bericht enthält sodann eine gute Übersicht über **Hindernisse der Cloud-Nutzung** (Bericht Bedarfsabklärung, S. 19). In Interviews sind die folgenden Themen, welche die Organisationen in ihrer Cloud-Nutzung einschränken, genannt worden: Rechtliche Grundlagen für eine Nutzung von Cloud-Leistungen werden als unklar wahrgenommen; viele unterschiedliche Stellen innerhalb der Organisation sind einzubeziehen; der Datenschutz und die damit beauftragten Stellen behindern bisweilen die Innovation. Insgesamt seien die Hindernisse vermutlich zwei Bereichen geschuldet: einerseits den ungenügenden Rahmenbedingungen und dem ungenügenden Wissen in der Organisation, um Cloud-Leistungen nutzen zu können und andererseits der mangelnden Klarheit, Cloud-Leistungen sicher und juristisch angemessen einzusetzen.

Während die diffusen Unsicherheiten bei vielen kantonalen und kommunalen Behörden zu einer gewissen Zurückhaltung und einer abwartenden Haltung zu führen scheinen, haben einzelne Behörden nach detaillierter Prüfung der rechtlichen Voraussetzungen, der technischen Möglichkeiten sowie des Sicherheitsdispositivs den **Schritt in die Cloud bereits vollzogen**. So nutzen beispielsweise der Kanton Basel-Stadt<sup>1</sup>, die Gebäudeversicherung Bern<sup>2</sup> sowie die Stadt Zug<sup>3</sup>, das Kantonsspital Baden<sup>4</sup> oder auch die Gemeinden Mumpf im Kanton Aargau und Bülach im Kanton Zürich schon heute die Cloud-Dienste von Microsoft (siehe dazu den Beitrag «Alles Gute zum Geburtstag: Ein Jahr Microsoft Cloud in der Schweiz, für die Schweiz» sowie «Digital-/ICT-Strategie Stadt Bülach»). Und dies, obwohl die Datenschutzgesetze in den jeweiligen Kantonen nicht weniger streng sind als in den übrigen (siehe hierzu die Übersicht der Datenschutzerlasse des Bundes und der Kantone im Anhang).

Das vorliegende White Paper hat zum Ziel, einen Beitrag zur Überwindung von fehlendem Wissen und rechtlichen Unklarheiten zu leisten, wobei der Fokus auf der Cloud-Nutzung durch Kantons- und Gemeindebehörden liegt.

1 <https://news.microsoft.com/de-ch/2020/06/10/weitere-azure-services-sowie-power-bi-aus-den-schweizer-datencenter-verfuegbar/>

2 <https://news.microsoft.com/de-ch/2021/05/25/die-gebaeudeversicherung-bern-und-ihre-tochtergesellschaften-vertrauen-auf-die-microsoft-Cloud-in-der-schweiz/>

3 <https://customers.microsoft.com/en-us/story/1363955807430340962-stadtzug-novacpta-teams>

4 <https://news.microsoft.com/de-ch/2021/05/18/kantonsspital-baden-und-heypatient-ag-kollaborieren-fuer-Cloud-basierten-gesundheitsbegleiter/>

## B. CLOUD ALS CHANCE FÜR DIE DIGITALISIERUNG

Die Vorteile für Behörden liegen auf der Hand: Cloud-Lösungen können einen Beitrag zur Umsetzung von Digitalisierungsinitiativen auf kommunaler, kantonaler und nationaler Ebene leisten und die Innovationskraft kann gestärkt werden.

Cloud-Lösungen können Behörden befähigen ihre Effizienz zu steigern und moderne Dienstleistungsangebote der Öffentlichkeit zur Verfügung zu stellen. Gerade auch kleineren Behörden und Gemeinwesen der kantonalen und kommunalen Stufe bietet der Wechsel zu einer Cloud-Lösung auch Möglichkeiten zur Verbesserung der Sicherheit und Compliance:

### a. Erhöhte Sicherheit

Die grossen Skaleneffekte, mit denen Microsoft arbeitet, geben die Möglichkeit, schnell erstklassige Sicherheitsmaßnahmen in die Cloud-Lösungen zu integrieren. Es ist keine Überraschung, dass viele auch grössere Kunden aus dem internationalen Behördenumfeld durch den Einsatz von Microsoft Sicherheitslösungen Möglichkeiten finden, das Gesamtrisiko für ihre Prozesse und Dienstleistungen zu reduzieren, insbesondere wenn sie einen 1:1-Vergleich mit ihrer bestehenden (nicht immer optimal gesicherten) lokalen IT-Umgebung vornehmen. Man sieht mehr und mehr, dass die Sicherheit ein starkes Argument für einen Cloud-Business-Case wird und nicht etwa das Problem darstellt.

### b. Compliance-Verbesserungen

Die Kosten der Gemeinwesen für die Einhaltung von Vorschriften sind in den letzten Jahren mit der Veröffentlichung mehrerer neuer Vorschriften auf nationaler und kantonaler Ebene deutlich gestiegen. Diese Vorschriften definieren strenge Anforderungen, die nicht immer leicht einzuhalten sind, und viele Behörden kämpfen damit, die Lücken für ihre lokalen IT-Umgebungen zu schliessen. Die Cloud-Dienste von Microsoft bieten eine breite Palette integrierter Compliance-Funktionen, die es Behörden ermöglichen, durch den Wechsel in die Cloud ihr gesamtes Compliance-Niveau strukturell zu erhöhen und dabei auch die ständig steigenden Kosten für Investitionen in Compliance-Massnahmen vor Ort zu sparen.

## c. Höhere Zuverlässigkeit und Ausfallsicherheit

Cloud-Lösungen basieren oft auf der neuesten Technologie in Kombination mit einem hohen Grad an Service-Automatisierung. Dies führt dazu, dass Cloud-Anbieter typischerweise ein sehr hohes Mass an Serviceverfügbarkeit über mehrere Verfügbarkeitszonen weltweit anbieten. Durch die Nutzung dieser Cloud-Technologien ergeben sich Möglichkeiten, Dienste fehlertoleranter und ausfallsicherer zu machen.

## C. HERAUSFORDERUNGEN

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 – eventuell im Ausland, 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.

Der Ausgangspunkt für dieses White Paper ist darum insbesondere die Frage, wie Microsoft als Cloud-Service-Provider mit den Herausforderungen umgeht, die sich ergeben wenn Kunden aus dem kantonalen und kommunalen Behördenumfeld sich für die Nutzung von Microsoft Online Services entscheiden.

Der Inhalt basiert auf Erfahrungen, die in zahlreichen Gesprächen mit kantonalen und kommunalen Behörden in der Schweiz gesammelt werden durften. Die Informationen sind weitgehend auch für private Organisationen relevant, wurden aber speziell auf die Bedürfnisse des öffentlichen Sektors ausgerichtet.



## 1. Kontrolle von Daten als Kernthema

Cloud-Lösungen zielen darauf ab, dass Daten anstatt auf eigenen lokalen Computern oder Servern auf entsprechenden Infrastrukturen von spezialisierten Drittanbietern wie bspw. Microsoft bearbeitet werden. Im Allgemeinen ist eine solche Datenbearbeitung durch Dritte grundsätzlich rechtlich zulässig unter der Voraussetzung, dass nebst der Einhaltung der fallspezifischen Compliance-Anforderungen insbesondere auch sicher gestellt 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 Anforderung des für die Daten Verantwortlichen 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 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 Information 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. Das Shared Responsibility Modell

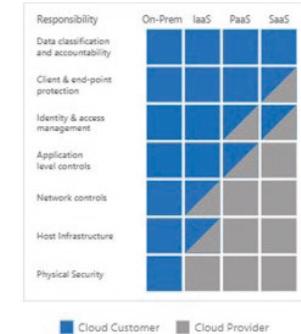
Die Ausprägung resp. die Organisation der Kontrolle bzw. den «Mix» und das Zusammenspiel der verschiedenen Instrumente zur Ausübung von Kontrolle unterscheidet sich je nach Integrationstiefe der beigezogenen Cloud-Lösungen. Dies wiederspiegelt sich auch in der Verteilung der Verantwortung und der Kosten 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 nur eine Partei für einen bestimmten Aspekt verantwortlich ist.



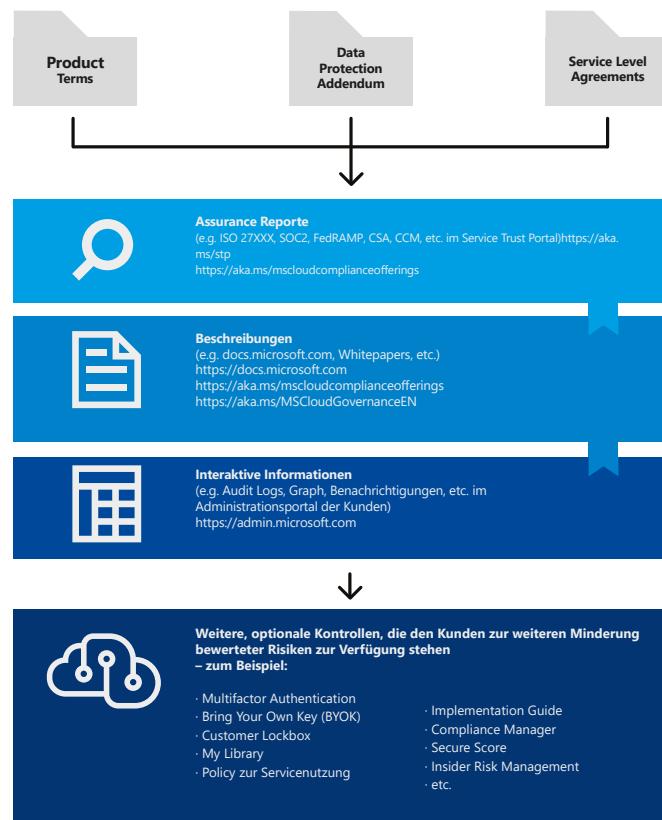
A risk assessment is not limited to the Cloud Provider, but focuses on the end-to-end process or service.



Damit einhergehend findet bei Cloud-Lösungen eine gewisse Verlagerung der Kontrollfunktion dahingehend statt, dass die organisatorischen resp. operationellen Aspekte der Kontrolle an Bedeutung zunehmen. Soweit 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).

### 3. Ausübung von Kontrolle in der Cloud

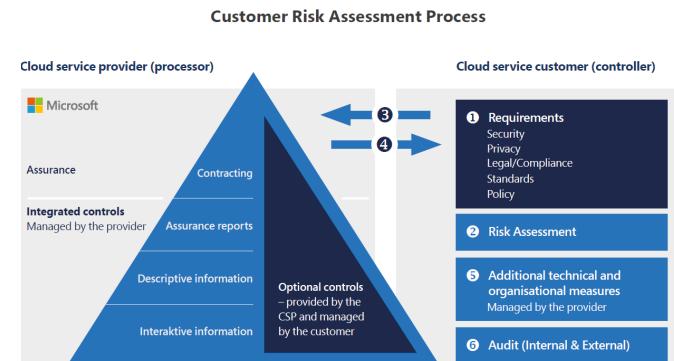
Um das notwendige Verständnis und die Einsicht zu erlangen, die den Ausgangspunkt für den Nachweis der Kontrolle bilden, ist es unerlässlich, die Gesamtstruktur der Microsoft Cloud-Vereinbarungen, der Dokumentation, der Anleitungen und nicht zuletzt der Zertifizierungen und Auditberichte zu kennen. Hier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



1. Die oberste Ebene bildet das abzuschliessende **Vertragswerk mit Microsoft**. Dies beinhaltet u.a. die **Universal Licence Terms**, in der die Datenbearbeitungsvereinbarung (für Microsoft Cloud genannt **Data Protection Addendum**) enthalten ist.
2. 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.
3. 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.
4. Schliesslich haben Kunden Zugriff auf fortlaufende Dokumentation und Informationen speziell zur Nutzung von Microsoft Cloud-Diensten, die über ein individuelles **Cloud-Service Verwaltungsportal** zur Verfügung stehen.

Für alle diese vier Ebenen von «Assurance Reports» 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 Kontrolle beim Kunden. Der Zusammenhang ist im folgenden Prozessmodell dargestellt:



## II. RECHTLICHE HERAUSFORDERUNGEN

### A. ÜBERSICHT

#### 1. Einleitung

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 insbesondere 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, S. 28).

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.

Gerade auf kantonaler Stufe bestehen zudem zahlreiche Merkblätter der kantonalen Datenschutzbehörden und der Konferenz der Schweizer Datenschutzbeauftragten, welche verschiedene Handlungsempfehlungen enthalten, die jedoch lediglich Empfehlungen darstellen.

#### 2. 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 meisten kantonalen Datenschutzgesetzgebungen vor.

Cloud-Lösungen sollten aber von klassischen Outsourcing-Lösungen unterschieden werden, welche ebenfalls als Auslagerungssachverhalt nach den einschlägigen kantonalen 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 respektive gar die in den Daten gespeicherten Informationen der Behörde inhaltlich erstellt, prozessiert oder verändert. 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 jedoch flüssig; Regelungen zum «Outsourcing» können darum auch auf den Fall von Cloud Computing-Konstellationen anwendbar sein. Es ist aber im Einzelnen genau zu prüfen, ob dies auch sachlich gerechtfertigt ist.

Generell ist die Erbringung von Informatikdienstleistungen keine genuin hoheitliche Aufgabe, auch wenn im Einzelfall die Daten selber, welche in Informatikdiensten von Dritten bearbeitet und gespeichert werden, die hoheitliche Aufgabenerfüllung erfüllen. Die Auslagerung von Informatikdiensten ist verwaltungsrechtlich grundsätzlich zulässig.

#### 3. 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).

### B. DATENSCHUTZRECHTLICHE REGELUNGEN IN BUND UND KANTONEN

#### 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. Sie sind dabei aber an die Vorgaben des Bundesrechts, insbesondere an das Recht auf Schutz vor Missbrauch persönlicher Daten (Art. 13 Abs. 2 BV) und des Völkerrechts gebunden.

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).

Die wesentlichen Bestimmungen der kantonalen Datenschutzerlasse sowie des Bundes sind in der Übersicht im Anhang zusammengestellt.

#### 2. Datenbearbeitung durch Dritte im Auftrag

In 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 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 in den kantonalen Datenschutzgesetzen vergleichbar mit der Rechtslage für Private (nach dem Datenschutzgesetz des Bundes).

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. Auch dieses Grundprinzip entspricht insoweit den Grundregeln des Datenschutzgesetzes des Bundes.

### 3. Die gängigsten Vorgaben im Einzelnen

#### a. 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 vereinbart werden sollen.<sup>5</sup>

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 grundsätzlich nicht möglich.

Die standardisierten Bedingungen können von Behörden als Hindernis für die Einführung von Cloud Lösungen wahrgenommen werden. Microsoft geht auf diese Herausforderung ein, indem Microsoft spezielle Vertragsänderungen anbietet, die auf die spezifischen Bedürfnisse von kantonalen und kommunalen Behörden zugeschnitten sind. Bitte kontaktieren Sie Ihren Microsoft Ansprechpartner oder Microsoft Partner, der Ihnen gerne weiterhilft.

#### b. Bearbeitung nach Weisung und im Interesse des öffentlichen Organs

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

Die Datenschutzbestimmungen von Microsoft<sup>6</sup> 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 dokumentierten 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.

#### c. Einbezug weiterer Datenbearbeiter

Der Bezug von Unterauftragsbearbeitern durch den Cloud-Anbieter ist nach den einschlägigen national und kantonalen Vorschriften grundsätzlich zulässig, sofern die Einhaltung der Pflichten des Cloud-Anbieters aus dem Auftragsbearbeitungsvertrag auch bei Unterbeauftragung sichergestellt ist. Nach neuem nationalen Datenschutzrecht (Art. 9 Abs. 3 revDSG) werden Cloud-Anbieter gesetzlich dazu verpflichtet, Kunden über den Bezug neuer oder den Ersatz bisheriger Subunternehmer als Unterauftragsbearbeiter zu informieren und ihnen zu ermöglichen, dem Bezug zu widersprechen, was auch durch das Einräumen eines Kündigungsrechts erreicht werden kann.

5 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](#))

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

Die Datenschutzbestimmungen von Microsoft<sup>7</sup> beschreiben 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 in den Datenschutzbestimmungen erfüllen.

Das Service Trust Center<sup>8</sup> führt die Liste, einschliesslich der von ihnen erbrachten Dienste, des Standorts ihres Hauptsitzes und des Umfangs und der Bedingungen, unter denen Unterauftragnehmer auf Kundendaten zugreifen können: <http://aka.ms/mscloudsubprocessors>.

Weder Microsoft noch Unterauftragnehmer haben 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 «Lock-box») 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 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, die sog. «Customer Lockbox»<sup>9</sup>.

#### d. Datensicherheit

Kantonale 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 Erlasses 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.

Alle Microsoft Onlinedienste bauen auf einer virtualisierten Umgebung auf. Virtualisierung und skalierbare IT-Infrastrukturen führen dazu, dass die physische Ebene der Computing-Einheiten getrennt wird von der Nutzungsebene, welche der Cloud-Kunde sieht. Die Hardware ist so aufgesetzt, dass ein Zugang der Benutzerinstanzen (auch «Virtual Machines») auf die Hardware nicht möglich ist (sog. «Isolierung» der Virtual Machine). Diese Isolierung sorgt für Sicherheit in der Abgrenzung der Benutzerinstanz sowie von darauf laufenden Applikationen von den zentralen Funktionen des Betriebssystems auf der Hardware. Außerdem führt diese Architektur dazu, dass Benutzer aus den Applikationen keine Befehle zum Lesen, Schreiben oder Ausführen auf dem darunterliegenden Host-System ausführen können.

Microsoft setzt darüber hinaus Methoden ein, damit aus der Benutzerinstanz eines Cloud-Kunden nicht auf zentrale Bereiche (namentlich den Speicherbereich) von Benutzerinstanzen eines anderen Kunden zugegriffen werden kann. Dies führt dazu, dass die im Rahmen einer sog. «Public Cloud» genutzten IT-Infrastrukturen nicht zu einer Beeinträchtigung der Kontrolle des Cloud-Kunden führen. Zentral ist, dass in den für den Cloud-Kunden zum Einsatz kommenden virtuellen Netzwerken in der Microsoft-Cloud nur eindeutige (jeweils nur für einen Cloud-Kunden verwendete) Zugangsdefinitionen zum Einsatz kommen.

Weitere typischerweise nur in einer Cloud-Umgebung vorkommende Sicherheitsaspekte erhöhen den Schutz von Daten gegen den Zugriff von Dritten zusätzlich: Aktualisierungen auf den Betriebssystemen und den Plattformsoftwares (sog. «Patching», d.h. Nachlegen von Softwarecode auf eine bestehende Softwareinstallation, um die bestehende Installation zu verbessern bzw. diesbezügliche Fehler zu beheben) erfolgen in der Regel automatisiert, d.h. ohne, dass Einwirkungen durch Menschen erforderlich wären. Microsoft hat weitere Schutzmassnahmen eingerichtet, namentlich Massnahmen organisatorischer Natur (Logging von logischen Zugriffen, Mitarbeiterprozesse, etc.).

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

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

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

9 <https://aka.ms/msazurelockbox> und <https://aka.ms/o365CustomerLockbox>

Über das Microsoft Trust Center<sup>10</sup> sowie über die Dienstüberprüfung im Security & Compliance Center<sup>11</sup> 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 (siehe oben Ziffer II.C.3). Auf diesem Weg kann sich der Cloud-Kunde jederzeit von der Einhaltung der Sicherheitspflichten durch Microsoft überzeugen.

#### e. Auslandsbezüge

Einige kantonalen Datenschutzgesetze stellen besondere Anforderungen an Projekte auf, in deren Rahmen die Verlagerung von Daten ins Ausland geplant ist. Insgesamt sind die diesbezüglichen Regeln aber durchaus vergleichbar mit jenen, die auch unter dem Datenschutzgesetz des Bundes (DSG) gelten.

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 einer Vielzahl von Services werden ausschliesslich in diesen Rechenzentren gespeichert. Falls innerhalb einer Region weitere Länder dazu kommen, wird Microsoft dies einen Monat im Voraus dem Cloud-Kunden anzeigen. Die jeweiligen konkreten Datenhaltungsstandorte können für jeden Onlinedienst über die jeweilige Dienstüberprüfung im Security & Compliance Center<sup>12</sup> abgerufen werden.

Die Anforderungen zur Bereitstellung der Onlinedienste kann es im Einzelfall notwendig machen, dass einige Kundendaten an Mitarbeiter oder Subunternehmer von Microsoft ausserhalb dieser primären Speicherregion zugänglich gemacht werden. Ebenfalls könnte 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 Zugriff auf Systeme oder Daten benötigen, um ein Problem lösen zu können.

Gemäss den Datenschutzbestimmungen für Onlinedienste darf deshalb Microsoft Daten, die Microsoft im Namens des Cloud-Kunden bearbeitet, grundsätzlich im Ausnahmefall auch in andere Ländern (mitunter auch in die USA), übertragen. 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.

Für den Fall eines solchen potentiellen Auslandsbezugs ausserhalb des EU/EWR-Raums hat Microsoft folgende Massnahmen getroffen: Für sämtliche Übermittlungen von Kundendaten, Professional Services-Daten und personenbezogenen Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz zur Bereitstellung der Produkte und Services gelten die von Microsoft implementierten EU-Standardvertragsklauseln. Microsoft hält sich an die datenschutzrechtlichen Anforderungen des Europäischen Wirtschaftsraums und der Schweiz in Bezug auf die Erhebung, Nutzung, Übermittlung, Speicherung und sonstige Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz.



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

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

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

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 prinzipien-treuen und strengen Ansatz im Umgang mit behördlichen Anfragen nach Zugriff auf Kundendaten, die sich im Gewahrsam von Microsoft befinden.<sup>13</sup> Microsoft veröffentlicht alle sechs Monate einen sog. «Law Enforcement Request Reports» um Transparenz über den Umfang und die Art dieser Vorfälle zu gewährleisten.<sup>14</sup> Die Berichte und können zur Unterstützung bei der Durchführung der gesetzlichen Risikobewertung herangezogen werden. Microsoft interagiert täglich 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.<sup>15</sup> 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.

Microsoft bietet zudem Vertragsänderungen an, die auf die spezifischen Bedürfnisse von kantonalen und kommunalen Behörden zugeschnitten sind. Bitte kontaktieren Sie Ihren Microsoft Ansprechpartner oder Microsoft Partner, der Ihnen gerne weiterhilft.

#### 4. Geheimhaltungsvorschriften

Eine strafbare Offenbarung im Sinne der strafrechtlichen Vorschriften zum Amts- und Berufsgeheimnis (insb. Art. 320 und Art. 321 StGB) liegt vor, wenn ein Aussenstehender die zu schützende Information (z.B. Amtsgeheimnisrelevante Informationen) tatsächlich wahrgenommen hat. Dieses tatsächliche Wahrnehmen kann im digitalen Kontext auch als «Klartextzugriff» bezeichnet werden. Offenbaren bedeutet «Zugänglichmachen» von Informationen, d.h. Angaben, die für sich «sprechend» sind und konkret eingesehen werden. Bei vielen Public-Cloud-Services finden indes generell keine derartigen Offenbarungen statt.

In gewissen Ausnahmesituationen kann ein höchst eingeschränkter und durch organisatorische Massnahmen abgesicherter und überwachter Zugriff auf Kundendaten notwendig sein, um die Onlinedienste für den Kunden betreiben zu können, zum Beispiel in gewissen Supportszenarien oder im Falle von kritischen Sicherheitsvorfällen.

Die betrieblichen Prozesse, die den Zugriff auf Kundendaten in Microsoft Onlinediensten regeln, sind durch technische und organisatorische Massnahmen geschützt, die starke Authentifizierung und Zugriffskontrollen, sowohl physisch als auch logisch, umfassen. Microsoft prüft proaktiv Zugriffskontrollen auf allen Ebenen der Onlinedienste. Microsoft Onlinedienste sind so konzipiert, dass die Techniker von Microsoft in der Lage sind den Onlinedienst zu betreiben und zu warten, ohne auf Kundendaten zuzugreifen. Microsoft-Mitarbeiter haben keinen ständigen Zugriff auf Kundendaten. Wenn ausnahmsweise Zugriff für den Dienstbetrieb erforderlich ist, werden rollenbasierte Zugriffskontrollen verwendet, um sicherzustellen, dass der Zugriff für einen angemessenen Zweck, für eine begrenzte Zeit und unter Aufsicht des Managements genehmigt wird.

Unsere Kunden vertrauen darauf, dass wir ihre Privatsphäre und die uns anvertrauten Daten schützen und die Informationen nur in der erwarteten Weise nutzen. Um diesem Anspruch gerecht zu werden, gehen wir weitreichende vertragliche Verpflichtungen gegenüber unseren Kunden ein. Microsoft ist sich bewusst, dass Kundendaten möglicherweise speziellen Geheimnisregeln unterliegen. Daher hält sich Microsoft strikt an ihre Vertraulichkeitsverpflichtungen gemäss den anwendbaren Kundenverträgen.

#### 5. 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.

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

14 Hier zu finden: <https://aka.ms/msler>

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

### III. HÄUFIGE FRAGEN UND ANTWORTEN

#### 1. Datenherrschaft; gibt es eine klare Definition und Vereinbarung bezüglich der Herrschaft des Kunden über seine Daten?

Ja. Im **Datenschutznachtrag zu den Produkten und Services von Microsoft** (engl. **Data Protection Addendum, DPA<sup>16</sup>**) steht auf Seite 6 unter «Art der Datenverarbeitung; Eigentumsverhältnisse» folgendes dazu:

«Microsoft wird Kundendaten, Professional Services-Daten und personenbezogene Daten nur wie nachstehend beschrieben und eingeschränkt nutzen und anderweitig 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. **Unter den Parteien behält sich der Kunde alle Rechte, Ansprüche und Eigentum an und für Kundendaten und Professional Services-Daten vor.** Microsoft erwirbt keine Rechte an den Kundendaten oder Professional Services-Daten, mit Ausnahme der Rechte, die der Kunde Microsoft in diesem Abschnitt gewährt.»

Die Einhaltung dieser Grundsätze wird durch die Übernahme des internationalen Standards **«ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud»** dokumentiert.<sup>17</sup>

Microsoft war zudem einer der ersten Cloud-Service-Provider, der die ISO/IEC 27701 Zertifizierung **«Privacy Information Management System»** erhalten hat.<sup>18</sup>

#### 2. Datenstandort; ist jederzeit klar, wo die Daten des Kunden gespeichert sind und wo sich die Rechenzentren befinden?

Der Abschnitt «Datenübermittlungen und Speicherstelle» im DPA<sup>19</sup>, Seite 10, beschreibt dies. Weitere - und spezifischere - vertragliche Verpflichtungen zum Datenaufenthalt sind hier aufgeführt: <https://www.microsoft.com/licensing/terms/de-DE/product/PrivacyandSecurityTerms/all>

Der Kunde kann seine Nutzung der Azure Cloud Dienste so konfigurieren, dass die Daten der meisten Services nur innerhalb der Schweiz oder der EU gespeichert werden. Insgesamt werden nach derzeitigem Stand mehr als 60 Regionen angeboten, darunter zwei in der Schweiz sowie mehrere innerhalb der EU. Eine vollständige Übersicht über die Standorte der Microsoft Cloud Datencenter findet sich in dieser interaktiven Karte: <https://aka.ms/azuredatalresidency>, für Office 365 hier: <https://aka.ms/o365dataresidency> und für Dynamics365 hier: <https://aka.ms/D365dataresidency>

Die meisten der verfügbaren Cloud-Dienste bieten Datenstandorte innerhalb der EU an (und eine wachsende Anzahl in der Schweiz): <https://azure.microsoft.com/de-de/global-infrastructure/services/> und für Office 365 Services hier: <https://aka.ms/mso365datalokation>

Die folgende Website bietet ferner spezifische Details zur Datenresidenz für M365 innerhalb der EU: <https://docs.microsoft.com/de-ch/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide>. Microsoft 365-Kunden können die Datenstandorte auch über ihr Microsoft 365 Admin Center überprüfen, indem sie zu Einstellungen | Organisationen | Organisationsprofil | Datenstandort navigieren.

Für Microsoft Azure ist eine Liste aller Dienste, die ausserhalb der EU-Regionen angeboten werden, hier aufgeführt: <https://azure.microsoft.com/de-de/global-infrastructure/services/> und die Datenresidenzverpflichtungen finden sich hier: <https://azure.microsoft.com/de-de/global-infrastructure/data-residency/>

Weitere Details zur Datenresidenz finden sich in den folgenden Whitepapers:

- Microsoft Azure: <https://azure.microsoft.com/de-de/resources/achieving-compliant-data-residency-and-security-with-azure/>
- Microsoft Dynamics: <https://aka.ms/d365dataresidencyWP>

Einige «nicht-regionale Dienste» werden aufgrund ihres Designs und ihrer Funktion ohne Verpflichtung auf einen bestimmten Datenstandort angeboten. Insbesondere zählt hierzu das Azure Active Directory Service (AAD), welches von zentraler Bedeutung für viele Onlinedienste ist. Auch für diesen Dienst werden indes gewisse Zusicherungen bezüglich Datenstandort gemacht, welche hier gefunden werden können: <https://aka.ms/msaadddatalocation>. Kunden sollten auf die Art der Daten achten, welche im AAD gespeichert werden.<sup>20</sup>

16 <https://aka.ms/dpa>

17 Siehe: <https://aka.ms/msiso27018> und: <https://docs.microsoft.com/de-ch/compliance/regulatory/offering-ISO-27018?view=o365-worldwide>

18 Siehe: <https://docs.microsoft.com/de-ch/azure/compliance/offering-is0-27701>

19 FN 16

20 Siehe: <https://docs.microsoft.com/de-de/azure/active-directory/hybrid/reference-connect-sync-attributes-synchronized>

Für einige Onlinedienste verweist Microsoft für weitere Details zum Datenstandort auf gewisse Abschnitte des Microsoft Trust Centers. Da die Microsoft Onlinedienste aus mehreren spezifischen Diensten bestehen und im Laufe der Zeit neue (Unter-)Dienste hinzugefügt werden können, verwendet Microsoft diesen Mechanismus des Verweises auf die Trust Center Landing Pages für aktuelle Informationen über die tatsächlichen Datenstandorte. Es ist hier wichtig zu beachten, dass obschon Microsoft den Inhalt dieser Webseiten von Zeit zu Zeit ändern kann, die Datenschutz- und Sicherheitsbedingungen zu den Onlinediensten<sup>21</sup> ausdrücklich festhalten, dass:

«(...) Microsoft keine Ausnahmen für vorhandene Dienste in der allgemeinen Version hinzufügen (...) [wird].»

Weiter wird im DPA<sup>22</sup> folgendes festgehalten:

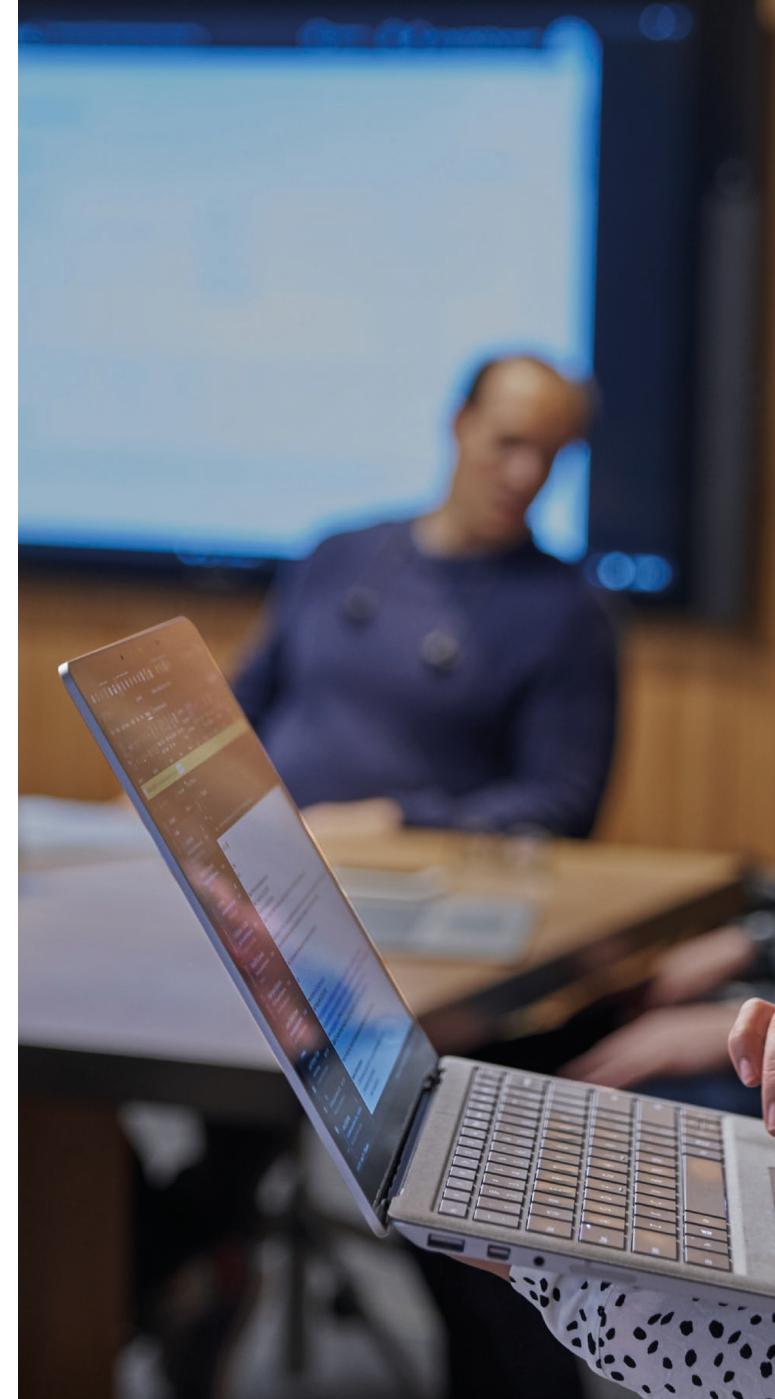
«Wenn der Kunde ein Produktabonnement verlängert oder ein neues Abonnement kauft oder einen Arbeitsauftrag für Professional Services eingeht, gelten die jeweils aktuellen DPA-Bestimmungen und bleiben während des Abonnements des Kunden für dieses Produkt oder die Laufzeit für diesen Professional Services unverändert.»

Folgende zusätzlichen kundenverwaltete Kontrollen sind in Bezug auf den Datenstandort verfügbar:

- Mit Hilfe von «Azure Policies»<sup>23</sup> kann der Kunde eigene Richtlinien für z.B. Compliance und allgemeine Sicherheitseinstellungen und -konfigurationen definieren. So können die Mindestanforderungen definiert werden, die bei der Bereitstellung und Nutzung eines Dienstes erfüllt werden müssen - z.B. Speicherort der Daten, Anzahl der privilegierten Konten, Firewall-Einstellungen etc.

- Die «Azure Blueprints»<sup>24</sup> ermöglichen es dem Kunden, sich vor Inbetriebnahme von Diensten, die nicht mit Datenspeicherung in der gewählten Region angeboten werden, zu schützen. Blueprints werden oft erstellt, um die Einhaltung eines relevanten Standards oder einer Spezifikation zu gewährleisten, wie z.B. der Blueprint der australischen Regierung ISM PROTECTED<sup>25</sup>.
- Kunden können eine «Customer Lockbox»<sup>26</sup> hinzufügen, um sicherzustellen, dass die endgültige Genehmigung von Szenarien mit potenziellem Fernzugriff auf Kundendaten bei einer durch den Kunden selbst benannten Ressource innerhalb der Kundenorganisation liegt.

Das als Schrems-II-Urteil bekannte Urteil des Europäischen Gerichtshofs hat Anlass dafür gegeben, die rechtlichen Grundlagen für Datentransfers und die mit den Datentransferszenarien verbundenen Risiken zu analysieren und die sog. «Ergänzenden Massnahmen» zur Minimierung solcher Risiken zu ergründen. Im Folgenden findet sich ein Beispiel dafür, wie eine solche Bewertung bei der Verwendung von Microsoft Azure-Dienste aussehen könnte.



21 Siehe: <https://www.microsoft.com/licensing/terms/de-DE/product/PrivacyandSecurityTerms/all>

22 FN 16

23 [https://docs.microsoft.com/de-ch/azure/governance/policy/tutorials/create-and-manage?WT.mc\\_id=msignitethtour2019-slides-afun80](https://docs.microsoft.com/de-ch/azure/governance/policy/tutorials/create-and-manage?WT.mc_id=msignitethtour2019-slides-afun80)

24 <https://aka.ms/azureblueprints>

25 <https://docs.microsoft.com/de-ch/azure/governance/blueprints/samples/ism-protected/control-mapping>

26 <https://docs.microsoft.com/de-ch/azure/security/fundamentals/customer-lockbox-overview>

## SCHRITT

## BESCHREIBUNG

### Mögliche Transferszenarien

#### Von Microsoft initiierte Wartung und Fehlerbehebung.

Von Microsoft initiierte Wartung und Fehlerbehebung.

Umstand des Transfers: Fernzugriff mit Privilegien, die möglicherweise Kundendaten für Wartungs- und Fehlerbehebungingenieure offenlegen.

Häufigkeit und Wahrscheinlichkeit: Die überwiegende Mehrheit der betrieblichen Aufgaben ist automatisiert, es finden keine Übertragungen statt. Gelegentlich können wichtige Aufgaben nicht automatisch ausgeführt werden und der Einsatz von Technikern ist erforderlich - die meisten dieser Szenarien erfordern keine Berechtigungen mit Zugriff auf Kundendaten. Nur eine Teilmenge dieser seltenen Fälle, in denen solche Privilegien erforderlich sind, umfasst den Fernzugriff aus Nicht-EU/EWR-Ländern.

Länder, aus denen in seltenen Fällen ein Fernzugriff erfolgen kann: USA, Australien, Japan, Kanada, Indien, Irland, Israel, Tschechische Republik, Deutschland, Serbien, Niederlande und Vereinigtes Königreich.

Zweck des Transfers: Wie auf Seite 6 des DPA<sup>27</sup> definiert, ist Zweck der Verarbeitung die Bereitstellung der Onlinedienste für den Kunden, welche folgendes umfasst:

- Die Bereitstellung von Funktionen wie vom Kunden und dessen Benutzern lizenziert, konfiguriert und verwendet werden, einschliesslich der Bereitstellung personalisierter Benutzererfahrungen;
- Die Fehlerbehebung (Verhinderung, Erkennung und Behebung von Problemen); und
- Die kontinuierliche Verbesserung (Installieren der neuesten Updates und Verbesserungen in Bezug auf Benutzerproduktivität, Zuverlässigkeit, Effektivität und Sicherheit).

Im Rahmen der Bereitstellung der Onlinedienste wird Microsoft Kundendaten oder personenbezogene Daten nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) Marktforschung zur Entwicklung neuer Funktionen, Dienstleistungen oder Produkte oder zu anderen Zwecken; es sei denn, eine solche Verwendung oder Verarbeitung erfolgt nach den dokumentierten Anweisungen des Kunden.

### Verwendeter Transfermechanismus

Sämtliche potenziellen Datenübertragungen, die im Rahmen der Microsoft Onlinedienste auftreten können, unterliegen den EU-Standardvertragsklauseln gemäss DPA<sup>28</sup>, wie sie auch für die Schweiz als geeignete Garantie anerkannt sind.

### Geeignetheit des Transfermechanismus

Gemäss Äusserungen des EDÖB im Nachgang zum Schrems-II-Urteil könnten die EU-Standardvertragsklauseln nicht ohne weiteres als genügende Garantien für gewisse Datentransfers erachtet werden, insbesondere mit Bezug zu Transfers in die USA. Im Falle gewisser Übertragungen resp. Fernzugriffen, sollten deshalb ergänzende Massnahmen geprüft werden.

### Können ergänzende Massnahmen ergriffen werden?

Ja, sowohl der Verantwortliche (Exporteur) als auch der Bearbeiter (Importeur) können ergänzende Massnahmen ergreifen.

27 FN 16

28 FN 16

---

**Geeignete ergänzende Massnahmen:**

Von Microsoft als Datenbearbeiterin: Zusätzlich zu den im DPA<sup>29</sup> bereits zugesicherten Kontrollen (insb. Anhang A – Sicherheitsmassnahmen; Anhang C – Nachtrag zu zusätzlichen Schutzmassnahmen; Anlage 2 – Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union) werden für betriebliche Aufgaben die folgenden Kontrollen vorgenommen:

- Der produktive Zugriff ist auf isolierte Identitäten und streng kontrollierte Arbeitsstationen limitiert.
- Zugriffe werden auf Basis einer rollenbasierten Zugriffskontrolle gewährt.
- Multi-Faktor-Authentifizierung ist erforderlich.
- Just-In-Time «JIT» stellt sicher, dass höhere Zugriffsrechte nur temporär und mit den geringstmöglichen Rechten erteilt werden.
- Zugriffsanfragen werden geprüft, protokolliert und überwacht, und riskante Erhöhungen werden gemeldet.
- Überwachung 24x7x365 durch das Microsoft Cyber Defense Operations Center.
- Alle Daten werden im Ruhezustand und bei der Übertragung verschlüsselt. Gemäß DPA<sup>30</sup> wird Microsoft Dritten Folgendes nicht bereitstellen:  
«a) einen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf verarbeitete Daten; (b) für die Sicherung der verarbeiteten Daten verwendete Verschlüsselungsschlüssel für die Plattform, oder die Möglichkeit, eine solche Verschlüsselung zu umgehen; (...)»

Von Microsoft als Importeurin:

- Die Microsoft Corporation hat eine langjährige Verpflichtung zum Datenschutz: <https://aka.ms/MSCloudPrivacy>
- Microsoft hat sich über viele Jahre hinweg stark für das Recht der Kunden auf ihre eigenen Daten und das Recht auf Transparenz bei rechtlichen Anfragen zum Datenzugriff eingesetzt und rechtliche Kämpfe dazu ausgefochten (Beispiel: <https://aka.ms/MSSecrecyOrders>)
- Nach dem Schrems-II-Urteil hat Microsoft weitere Verpflichtungen zum Schutz von Kundendaten angekündigt (<https://aka.ms/MSdyd>) und diese Verpflichtungen in die Datenschutzbestimmungen aufgenommen.
- Die Prozesse und die Historie des Importeurs bei der Bearbeitung von Anfragen Dritter für den Zugriff auf Kundendaten ist unter <https://aka.ms/MSLERH> und <https://aka.ms/MSLERR> abrufbar - aus diesen Berichten lässt sich ableiten, dass diese zusätzlichen Massnahmen des Importeurs die Wahrscheinlichkeit des Zugriffs auf Kundendaten über Microsoft Azure-Dienste effektiv auf «nahe Null» resp. «auf ein akzeptables niedriges Niveau» senken.

Vom Kunden als Verantwortlicher resp. Exporteur:

- Azure Customer Lockbox Service. Vor der Zuweisung von Privilegien, die potenziellen Zugriff auf Kundendaten ermöglichen, muss der Kunde die Zuweisung genehmigen. Mehr Details unter <https://aka.ms/msazurelockbox>
- Azure Policy Service. Effektive Einschränkung der Verfügbarkeit von Onlinediensten, auf diejenigen, die z.B. Datenresidenz innerhalb der Europa anbieten.
- Azure Überwachungsdienst. Log-Analyse und Benachrichtigung über Datenzugriffe.

---

**Reevaluation**

Microsoft stellt eine Governance-Struktur sowie unterstützende Technologien zur Verfügung, um alle oben genannten Elemente regelmässig zu überprüfen, insb.: Automatische Benachrichtigung über Änderungen an Dokumentationen, Audits, Zertifizierungen und Vereinbarungen mithilfe der My-Library-Funktion im Microsoft Services Trust Portal.

Azure Customer Lockbox, um eine fallweise Bewertung von Datenübertragungsszenarien während der Wartung, Fehlerbehebung und Supportinstanzen zu ermöglichen.

Azure Policy Service auf Tenant-Ebene, für eine richtliniengesteuerte Konfiguration und Erreichbarkeit ausschliesslich der relevanten Dienste.

Überwachung von Kunden-Audit-Protokollen.

**3. Wie werden Änderungen an der Sicherheits-, Datenschutz- und Compliance-Dokumentation, den Listen der Unterauftragnehmer, den Allgemeinen Geschäftsbedingungen usw. gehandhabt?**

Die gesamte Dokumentation wird auf dem «Service Trust Portal»<sup>31</sup> veröffentlicht, und der Kunde kann bestimmte Dokumente, Zertifikate und Audit-Berichte über die MyLibrary-Funktion auswählen, für welche er Benachrichtigungen über Änderungen wünscht.

**4. Hat der Kunde die Möglichkeit, Prüfungen selber durchzuführen oder durch eine unabhängige, akkreditierte und vom Kunden ausgewählte Prüfgesellschaft durchführen zu lassen?**

Ja. Im Abschnitt «Prüfung der Einhaltung» auf Seite 9 des DPA<sup>32</sup> sind die Prüfrechte des Kunden festgehalten inkl. unter welchen Bedingungen der Kunde eine spezielle Prüfung durch eine dritte Partei durchführen lassen kann.

**5. Wie werden die Audit-Logs gesichert? - Wie und wie oft werden sie zum Schutz vor unentdeckten Sicherheitsvorfällen überprüft?**

Microsoft bietet Überwachungs- und Protokollierungstechnologien, um Kunden maximale Transparenz über die Aktivitäten ihrer Cloud-basierten Netzwerke, Anwendungen und Geräte zu bieten und um potenzielle Sicherheitsschwachstellen zu identifizieren. Die Onlinedienste enthalten Funktionen, mit denen Kunden den Zugriff ihrer Mitarbeiter auf die Dienste einschränken und überwachen können, darunter das Azure AD Privileged Identification Management System und eine Multi-Faktor-Authentifizierung.

Darüber hinaus enthalten die Onlinedienste integrierte, von Windows genehmigte Windows PowerShell-Skripte, die Zugriffsprivilegien kontrollieren und damit die Möglichkeit einer Fehlkonfiguration minimieren.

Microsoft ermöglicht Kunden das Protokollieren von Zugriff und Nutzung der Informationssysteme, inkl. Registrierung der benutzten Zugriffs-ID, der Zeit, den gewährten oder verweigerten Berechtigungen sowie anderer relevanter Aktivitäten.

Ein internes, unabhängiges Microsoft-Team prüft das Protokoll mindestens einmal pro Quartal. Kunden haben Zugang zu diesen Audit-Protokollen.

Darüber hinaus überprüft Microsoft regelmässig die Zugriffsebenen, um sicherzustellen, dass nur Benutzer mit entsprechender Berechtigung Zugriff haben.

**6. Ist Microsoft eindeutig zur Einhaltung von Datenschutzgesetzen und -verordnungen verpflichtet?**

Ja. Gemäss Abschnitt «Einhaltung von gesetzlichen Regelungen» auf Seite 5 des DPA<sup>33</sup>:

*« Microsoft befolgt alle für die Bereitstellung der Produkte und Services durch Microsoft geltenden Gesetze und Vorschriften, einschliesslich Gesetzen zu Meldepflichten bei Sicherheitsverletzungen, sowie Datenschutzvorschriften.»*

Zudem hält sich Microsoft an die datenschutzrechtlichen Anforderungen des Europäischen Wirtschaftsraums und der Schweiz in Bezug auf die Erhebung, Nutzung, Übermittlung, Speicherung und sonstige Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz (Abschnitt «Datenübermittlungen und Speicherstelle - Datenübermittlungen», S. 10 DPA<sup>34</sup>).

**7. Erfüllt die Datenbearbeitungsvereinbarung die gesetzlichen Mindestanforderungen?**

Ja. Der Datenschutznachtrag<sup>35</sup> zu den Produkten und Services von Microsoft erfüllt sämtliche Anforderungen der nationalen und kantonalen Datenschutzgesetze.

Microsoft aktualisiert die Vereinbarung zudem regelmässig basierend auf dem Feedback von Kunden und Aufsichtsbehörden. Zum Beispiel hat das niederländische Justizministerium mehrere umfangreiche Datenschutzbewertungen durchgeführt, deren Ergebnisse den Kunden weltweit zur Verfügung gestellt wurden, siehe: <https://aka.ms/DutchPrivacyDPIA> und <https://news.microsoft.com/de-de/einfuehrung-von-mehr-datenschutz-transparenz-fuer-unsere-kommerziellen-cloud-kunden/>

**8. Kann Microsoft die «Exit-Strategie» eines Kunden unterstützen? - Wie?**

Ja. Nach Ablauf oder Kündigung kann der Kunde seine Daten extrahieren. Wie im DPA<sup>36</sup> beschrieben, wird Microsoft die im Onlinedienst gespeicherten Kundendaten in einer funktional eingeschränkten Version des Dienstes für 90 Tage nach Ablauf oder Beendigung des Abonnements des Kunden aufzubewahren. Der Kunde kann somit die Daten extrahieren. Wenn die 90-tägige Aufbewahrungsfrist abläuft, deaktiviert Microsoft das Konto des Kunden und löscht die Kundendaten maximal 180 Tage nach Ablauf oder Beendigung der Nutzung eines Onlinedienstes durch den Kunden.

<sup>31</sup> <https://servicetrust.microsoft.com>

<sup>32</sup> FN 16

<sup>33</sup> FN 16

<sup>34</sup> FN 16

<sup>35</sup> FN 16

<sup>36</sup> FN 16

Die 90 Tage nach Ablauf oder Beendigung sind als «Sicherheitsnetz» für eventuelle Restdaten gedacht. Wenn ein Kunde einen Exit benötigt oder plant, sollte einer der ersten Schritte in einem strukturierten Exit Plan nicht darin bestehen, das Abonnement einfach zu kündigen. Stattdessen sollte der Kunde einen koordinierten Datenextraktionsprozess starten in welchem ein neues Ziel für die Daten festgelegt wird. Microsoft bietet zusätzlich zum Standard-Mechanismus mehrere weitere Optionen für die Extraktion von Kundendaten an. Beachten Sie diesbezüglich auch die Ausführungen hierzu im DPA<sup>37</sup>:

*« Während der Laufzeit des Abonnements des Kunden oder der Inanspruchnahme von Professional Services durch den Kunden, hat der Kunde jederzeit die Möglichkeit, auf die in jedem Onlinedienst gespeicherten Kundendaten und Professional Services-Daten zuzugreifen, diese zu extrahieren und zu löschen. »*

Das Eigentum an Dokumenten, Aufzeichnungen und anderen Daten verbleibt beim Kunden und wird nicht an Microsoft oder eine andere Partei übertragen.

Microsoft hat zudem einen Leitfaden zur Gestaltung einer «Exit-Strategie» erstellt, der auf dem Service Trust Portal, unter dem Menüpunkt «FAQ and White Papers» gefunden werden kann<sup>38</sup>.

## 9. Gibt es Dokumentation darüber, wie die Onlinedienste betrieben, gesichert und gewartet werden?

Kunden haben jederzeit Zugriff auf ein aktualisiertes Portfolio von Zertifizierungen und Audits des Betriebs der Onlinedienste durch Dritte.

In einer öffentlich zugänglichen Zusammenfassung<sup>39</sup> wird zudem beschrieben, wie die Microsoft Cloud Infrastructure Organisation (MCIO) die hohe Zuverlässigkeit und Sicherheit der Cloud-Plattformen sicherstellt. Das Dokument ist global angelegt und umfasst Ausführungen zur physischen Readiness der Cloud-Infrastruktur, zu den robusten Incident-Management-Prozessen, dem Service-Support, zur generellen Sicherheitsarchitektur, dem Änderungsmanagement, zur Compliance, dem Hardware-Design der Rechenzentren, Netzwerke, Software sowie der Nachhaltigkeitsstrategie.

MCIO-Rechenzentren werden nach dem Konzept «Operational Security Assurance»<sup>40</sup> (OSA) betrieben, welches die Einbettung aller Einzelfahrungen mit Cybersicherheitsbedrohungen sicherstellt, die Microsoft über SDL, das Microsoft Security Response Center<sup>41</sup>, und das übergreifende Microsoft Cyber Defense Operations Center<sup>42</sup> sammelt. OSA minimiert somit Risiken, weil dadurch sichergestellt wird, dass die laufenden betrieblichen Aktivitäten strengen Sicherheitsrichtlinien folgen, und darüber hinaus validiert wird, dass die Richtlinien tatsächlich befolgt werden. Wenn Probleme auftreten, hilft ein gut etablierter Feedback-Loop sicherzustellen, dass künftige Überarbeitungen der OSA Abhilfemaßnahmen enthalten, um diese Probleme zu beheben. Auf diese Weise wird das OSA ständig weiterentwickelt, um das aktuelle globale Bedrohungsbild widerzuspiegeln.

Eine detaillierte Beschreibung des MCIO Information Security Management Systems (ISMS), das nach ISO (27001) zertifiziert ist, finden Sie hier: <https://aka.ms/MSISMS>

Schliesslich bieten die Microsoft Azure Security Fundamentals<sup>43</sup> Details zu den in die Plattform eingebauten Funktionen und ein Cloud Services Due Diligence Checklist Framework, welches sich an den internationalen Standards für Cloud Services Agreements orientieren (Standards wie ISO/IEC 19086, mit Verweis auf ISO/IEC 19941).

## 10. Inwieweit werden internationale Sicherheits- und Datenschutz-Standards unterstützt?

Das Portfolio an Standardzertifizierungen der Microsoft Onlinedienste ist der beste Ausgangspunkt für den Schutz sensibler und wichtiger Geschäftsinformationen. Die vollständige Liste der Standards, nach denen Microsoft Cloud zertifiziert ist, findet sich hier: <https://aka.ms/mscloudcomplianceofferings>

Die Grundlage bildet sicherlich die ISO27001-Zertifizierung<sup>44</sup> und darauf aufbauend ISO27018<sup>45</sup> (PII in Cloud) und ISO27701<sup>46</sup> (Privacy Information Management System oder PIMS).

Im Jahr 2014 wurde die ISO/IEC 27018:2014 als Ergänzung zur ISO/IEC 27001 verabschiedet und wurde damit zum ersten internationalen Code of Practice für Cloud-Datenschutz. Die Zertifizierung basiert auf dem EU-Datenschutzrecht und bietet Cloud-Service-Providern, die als Datenverarbeiter von personenbezogenen Daten (PII) agieren, spezifische Anleitungen zur Risikobewertung und zu Sicherheits- und Datenschutzkontrollen nach dem Stand der Technik zum Schutz von PII.

Microsoft war der erste grosse Anbieter von Hyperscale Cloud Computing, der die ISO27018-Zertifizierung anstrebe und erhielt.

37 FN 16

38 Siehe: [https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad\\_FAQ\\_and\\_White\\_Papers](https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_FAQ_and_White_Papers)

39 <https://aka.ms/mscloudoperations>

40 <https://aka.ms/msopsec>

41 <https://www.microsoft.com/de-de/msrc?rtc=1>

42 <https://www.microsoft.com/de-de/msrc/cdoc?rtc=1>

43 <https://docs.microsoft.com/de-ch/azure/security/fundamentals/technical-capabilities>

44 <https://aka.ms/mscloudiso>

45 <https://aka.ms/msiso27018>

46 <https://aka.ms/PIMS3pager>

Mindestens einmal pro Jahr wird die Microsoft Cloud Platform von einer akkreditierten Dritt-zertifizierungsstelle auf die Einhaltung von ISO/IEC 27001 und ISO/IEC 27018 überprüft. Dies bietet eine unabhängige Validierung, dass anwendbare Sicherheitskontrollen vorhanden sind und effektiv funktionieren.

Als Teil dieses Prozesses zur Überprüfung der Konformität bestätigen die Auditoren in ihrem «Statement of Applicability», dass die Cloud-Dienste und kommerziellen technischen Supportdienste von Microsoft ISO/IEC 27018-Kontrollen für den PII-Schutz enthalten.

Der neue internationale Standard ISO/IEC 2770175 Privacy Information Management System (PIMS) (während des Entwurfszeitraums als ISO/IEC 27552 bekannt), hilft Organisationen, die gesetzlichen Anforderungen an den Datenschutz einzuhalten. Der Standard umreiss einen umfassenden Satz von Betriebskontrollen, die auf verschiedene Vorschriften, einschliesslich der GDPR, abgebildet werden können. Nach der Zuordnung werden die PIMS-Betriebskontrollen von Datenschutzexperten implementiert und von internen oder externen Prüfern geprüft, was zu einer Zertifizierung und einem umfassenden Konformitätsnachweis führt. Unmittelbar nach der Veröffentlichung der ISO27701 im August 2019 hat Microsoft den Beginn der Zertifizierung beantragt und am 13. Januar 2020 bekannt gegeben, dass die Zertifizierung abgeschlossen ist.

Alle weiteren Details unter <https://aka.ms/MSComplianceDokumentation> und <https://aka.ms/mscloudprivacystandards>

Eine allgemeine Übersicht über den Zertifizierungsstand der Microsoft Cloud-Plattform findet sich hier:

<https://aka.ms/mscloudcomplianceofferings>

## 11. Wie wird die geografische Resilienz sichergestellt?

Die Microsoft-Cloud-Infrastruktur ist derzeit in mehr als 60 Regionen unterteilt, die zum Schutz vor externen, nicht digitalen Bedrohungen geografisch getrennt sind.

Kundendaten in Azure werden in der Region der Wahl gespeichert und dort mehrfach gespiegelt. In vielen Regionen gibt es mehr als zwei Rechenzentren, weshalb einige Dienste dediziert in diesen Regionen angeboten werden können, was die Ausfallsicherheit je nach geografischem Standort weiter erhöht.

Eine sehr viel detailliertere Beschreibung, wie man Data Residency in den Microsoft Azure Regionen aktiviert, findet sich im Whitepaper «Data Residency und Schutz von Daten in Microsoft Azure-Regionen»<sup>47</sup> vom April 2021. Dieses Papier enthält die notwendigen Informationen und Werkzeuge zur Optimierung von Datenstandort und Datenzugriff, inkl. einer detaillierten Darstellung der regionalen Azure-Infrastruktur, der Datenstandortgarantien pro Dienst und wie Kunden Datenstandort und -zugriff verwalten können.

Ebenfalls enthalten sind Informationen zum ExpressRoute-Dienst<sup>48</sup>, mit welchem Kunden lokale Netzwerke über eine private Verbindung, die von einem Konnektivitätsanbieter bereitgestellt wird, in die Microsoft Cloud erweitern können. Die Verbindung kann über ein Any-to-Any-Netzwerk (IP VPN), ein Point-To-Point-Ethernet-Netzwerk oder eine virtuelle Querverbindung über einen Konnektivitätsanbieter in einer Colocation-Einrichtung erfolgen. ExpressRoute-Verbindungen gehen nicht über das öffentliche Internet. Dadurch bieten ExpressRoute-Verbindungen konsistente Latenzen, grössere Zuverlässigkeit, schnellere Geschwindigkeiten und höhere Sicherheit als typische Verbindungen über das Internet.

## 12. Wie wird die Datenaufbewahrung gehandhabt?

Dies wird ausführlich beschrieben in CSA CCM23, Abschnitt «Data Governance».

Speziell für Microsoft 365 finden sich Details zur Datenaufbewahrung unter: <https://docs.microsoft.com/de-ch/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview?view=o365-worldwide>

Beachten Sie, dass der Kunde umfassende Kontrolle über die Datenaufbewahrung innerhalb der Microsoft Online Services hat.

Für Microsoft 365: <https://docs.microsoft.com/de-ch/microsoft-365/compliance/manage-information-governance?view=o365-worldwide>

Für Microsoft Azure: <https://docs.microsoft.com/de-ch/azure/purview/>  
Festplatten werden nicht wiederverwendet oder repariert.

## 13. Werden Penetrationstests sowohl für Netzwerke als auch für Anwendungen durchgeführt?

Ja. Microsoft führt regelmässig Penetrationstests durch, um eine kontinuierliche Verbesserung der Gesamtsicherheit und der «Incident Response»-Verfahren sicherzustellen. Diese internen Tests helfen den Sicherheitsexperten von Microsoft einen methodischen, replizierbaren und optimierten Schritt-für-Schritt-Reaktionsprozess sowie eine Automatisierung zu erreichen.

Berichte über Penetrationstests werden auf der Registerkarte «Pentest and Security Test» im Abschnitt Datenschutz im Security Trust Portal<sup>49</sup> veröffentlicht.

Darüber hinaus führt das sog. «Microsoft Red Team» Live-Penetrationstests gegen Microsoft Managed Cloud-Infrastrukturdienste und -Programme vor Ort durch. Diese simulieren «reale» Sicherheitsverletzungen und führen fortlaufende Übungen zur Sicherheitsüberwachung und zur Reaktion auf Vorfälle durch, um die Sicherheit in Microsoft Azure, Microsoft 365 und Dynamics 365 zu validieren und zu verbessern.

Diese Erfahrungen mit Sicherheitsverfahren bilden eine solide Grundlage für Kunden, um Cloud-basierte Lösungen sicher einzusetzen und zu verwalten.

47 <https://azure.microsoft.com/de-de/resources/achieving-compliant-data-residency-and-security-with-azure/en-us/>

48 <https://azure.microsoft.com/de-de/services/expressroute/>

49 <https://aka.ms/stp>

#### 14. Wie wird sichergestellt, dass der Kunde seine Daten im Falle von Fehlern oder Verlusten wiederherstellen kann?

Kundendaten werden kontinuierlich repliziert und mehrfach innerhalb der ausgewählten Region abgelegt. Dies ermöglicht die Wiederherstellung von Daten im Falle von Fehlern in dieser lokalen Infrastruktur. Es liegt in der Verantwortung des Kunden, weitere Schritte zu unternehmen, um zusätzliche Fehlertoleranz zu erreichen, z.B. historische Backups von Kundendaten zu erstellen, Backups von Kundendaten außerhalb der Cloud-Umgebung zu speichern, redundante «Compute Instances» in und zwischen den Rechenzentren zu implementieren oder den «Zustand» und die Daten in einer Virtual Machine zu sichern.

Microsoft bietet dem Kunden die Möglichkeit, diese Funktion z.B. auf Azure Storage aufzubauen. Zur Unterstützung der Due Diligence ist es erwähnenswert, dass die CSA CCM23 Control ID DG-04 Data Governance Retention Policy Folgendes fordert:

*«Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals.»*

In der Antwort von Microsoft, die im Dokument «Microsoft Azure Standard Response to RFI - Security & Privacy»<sup>50</sup> zu finden ist, steht Folgendes:

*«Data retention policies and procedures are defined and maintained in accordance with regulatory, statutory, contractual or business requirements. The Microsoft Azure backup and redundancy program undergoes an annual review and validation. Microsoft Azure backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Microsoft Azure includes replication features detailed below to help prevent loss of customer data in the event of failures within a Microsoft data center.»*

[...]

*Information back-up is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.5.1. For more information, review of the publicly available ISO standards we are certified against is suggested.»*

Darüber hinaus wird eine Georeplikation bereitgestellt, um die Daten im Falle einer grösseren Katastrophe im Rechenzentrum oder eines vorübergehenden Hardwareausfalls zu sichern. Der Kunde hat drei Optionen für die Replikation von Daten:

**Lokal-redundanter Speicher (LRS)** wird innerhalb eines Rechenzentrums dreimal repliziert. Wenn Daten in einen Blob, eine Queue oder eine Tabelle geschrieben werden, wird der Schreibvorgang synchron über alle drei Replikationen hinweg durchgeführt. LRS schützt Ihre Daten vor normalen Hardwareausfällen.

**Geo-redundanter Speicher (GRS)** wird innerhalb einer einzigen Region dreimal repliziert und zusätzlich asynchron in eine zweite Region repliziert, die Hunderte von Kilometern von der primären Region entfernt ist. GRS hält ein Äquivalent von sechs Kopien (Replikate) der Daten (drei in jeder Region). GRS ermöglicht ein Failover auf eine zweite Region, wenn die erste Region aufgrund eines grösseren Ausfalls oder einer Katastrophe nicht wiederhergestellt werden kann. GRS wird gegenüber lokal redundantem Speicher empfohlen.

**Georedundanter Speicher mit Lesezugriff (RA-GRS)** bietet alle oben genannten Vorteile des georedundanten Speichers und ermöglicht außerdem den Lesezugriff auf Daten in der sekundären Region für den Fall, dass die primäre Region nicht mehr verfügbar ist. Geo-redundanter Speicher mit Lesezugriff wird für maximale Verfügbarkeit mit zusätzlicher Dauerhaftigkeit empfohlen.

Eine Anleitung für Kunden, wie sie einen Backup- und Wiederherstellungsplan für Azure-Dienste erstellen, pflegen und testen können, der ihrer Toleranz gegenüber eingeschränkter Funktionalität während einer Katastrophe entspricht, findet sich unter <https://docs.microsoft.com/de-ch/azure/architecture/framework/resiliency/backup-and-recovery>

50 <https://aka.ms/MSzurecsa>



Bei SaaS-Lösungen wie Microsoft 365 verfügt die Plattform an sich bereits über eine eingebaute Datenresilienz<sup>51</sup>, dennoch sollten Kunden überlegen, wie sie ihre Daten am besten vor modernen Bedrohungen (z.B. Ransomware-Angriffen) schützen können, indem sie Lösungen zum Schutz vor Bedrohungen<sup>52</sup> und Wiederherstellungsoptionen<sup>53</sup> nutzen und ein Backup des Dienstes konfigurieren (z.B. bei Exchange Online<sup>54</sup>).

#### 15. In welchem Umfang wird Verschlüsselung verwendet in Bezug auf ruhende Daten («at rest») und für Daten «in transit»?

Gemäss DPA<sup>55</sup> werden

«Kundendaten und Professional Services-Daten (jeweils einschließlich aller darin enthaltenen personenbezogenen Daten), die über öffentliche Netzwerke zwischen dem Kunden und Microsoft oder zwischen Microsoft-Rechenzentren übertragen werden, werden standardmäßig verschlüsselt.

Microsoft verschlüsselt auch ruhende Kundendaten in Onlinediensten und ruhende Professional Services-Daten. Im Fall von Onlinediensten, in denen der Kunde oder ein Dritter, der im Namen des Kunden handelt, Anwendungen erstellen kann (z. B. bestimmte Azure-Dienste), kann die Verschlüsselung der in diesen Anwendungen gespeicherten Daten nach Ermessen des Kunden erfolgen, unter Verwendung von Funktionen, die von Microsoft bereitgestellt werden oder die der Kunden von Dritten erlangt.»

Kundendaten in den Enterprise Cloud-Diensten von Microsoft werden durch eine Vielzahl von Technologien und Verfahren, einschliesslich verschiedener Formen der Verschlüsselung, geschützt. Microsoft bietet mehrere integrierte Verschlüsselungsfunktionen, um den Schutz der Daten zu unterstützen:

- Für Microsoft 365 verwendet Microsoft kryptographische Industrie-standards wie TLS/SSL und AES, um die Vertraulichkeit und Integrität von Kundendaten zu schützen. Für Daten in transit handeln alle Server mit Kundenbesprechungen eine sichere Sitzung mit TLS/SSL mit Client-Rechnern aus, um Kundendaten zu schützen. Für Daten at rest installiert Microsoft 365 BitLocker mit AES 256-Bit-Verschlüsselung auf sämtlichen Servern, auf denen Nachrichtendaten, inkl. Mail- und Chat-Unterhaltungen, sowie alle Daten in SharePoint Online und OneDrive for Business gespeichert sind. Zusätzlich verfügt Microsoft in einigen Szenarien über eine Benutzerverschlüsselung auf Dateiebene.
- Bei Azure helfen technologische Sicherheitsmaßnahmen wie verschlüsselte Kommunikation und Betriebsprozesse, die Daten der Kunden zu schützen. Microsoft ermöglicht es Kunden auch zusätzliche Verschlüsselung zu implementieren und ihre eigenen Schlüssel zu verwalten. Für Transfertypen verwendet Azure sichere Transportprotokolle nach Industriestandard, wie TLS/SSL, zwischen Benutzergeräten und Microsoft-Rechenzentren. Für Daten im Ruhezustand bietet Azure viele Verschlüsselungsoptionen, wie z.B. die Unterstützung von AES-256, wodurch Kunden die Flexibilität erhalten, das Datenspeicherszenario zu wählen, das ihren Anforderungen am besten entspricht.
- Microsoft verwendet einige der stärksten und sichersten Verschlüsselungsprotokolle, die verfügbar sind, um Schranken für den unbefugten Zugriff auf Kundendaten zu schaffen. Eine ordnungsgemässen Schlüsselverwaltung ist ebenfalls ein wichtiges Element optimaler Verschlüsselungslösungen, und Microsoft stellt sicher, dass alle von Microsoft verwalteten Verschlüsselungsschlüssel ordnungsgemäss gesichert sind.

Die Validierung der Microsoft-Verschlüsselungsrichtlinie und ihre Durchsetzung wurde von mehreren unabhängigen Prüfern verifiziert, und die Berichte über diese Prüfungen sind auf dem Service Trust Portal<sup>56</sup> verfügbar.

Darüber hinaus bietet Microsoft 365 sog. «Customer Key Encryption», welche eine weitere Verschlüsselungsdimension auf Anwendungsebene hinzufügt: <https://docs.microsoft.com/de-ch/microsoft-365/compliance/customer-key-overview?view=o365-worldwide>

Spezielle Informationen zur Verschlüsselung:

- Wie Microsoft Cloud Platform Verschlüsselung generell einsetzt: <https://docs.microsoft.com/de-de/compliance/assurance/assurance-encryption>
- Microsoft Azure Verschlüsselung: <https://docs.microsoft.com/de-ch/azure/security/fundamentals/encryption-overview>
- Microsoft O365 Verschlüsselung: <https://docs.microsoft.com/de-ch/microsoft-365/compliance/encryption?view=o365-worldwide>
- <https://aka.ms/o365IntroTilKryptering>
- Mail-Verschlüsselung: <https://docs.microsoft.com/de-ch/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwide>
- Für eine schnelle Einführung in viele dieser Themen stehen auch Videos von Microsoft Security zur Verfügung:
- M365 Verschlüsselung von data-at-rest: <https://www.youtube.com/watch?v=Dk380mk-xh0&t=41s>
- Azure-Datenschutz: <https://www.youtube.com/watch?v=dRgZJpKj7hU&t=81s>

51 <https://docs.microsoft.com/de-ch/compliance/assurance/assurance-data-resiliency-overview>

52 <https://docs.microsoft.com/de-ch/microsoft-365/security/office-365-security/protect-against-threats?view=o365-worldwide>

53 <https://docs.microsoft.com/de-ch/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide>

54 <https://docs.microsoft.com/de-ch/exchange/back-up-email>

55 <https://aka.ms/dpa>

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

## 16. Hat der Kunde Zugriff auf zusätzliche Verschlüsselungstechnologien inkl. BYOK etc.?

Grundsätzlich verwaltet Microsoft die Schlüssel für die in den Onlinediensten eingesetzten starken Standardverschlüsselungen, aber Kunden können auch ihre eigene Verschlüsselung verwenden.

Aus vertraglicher Sicht gilt es darauf hinzuweisen, dass Microsoft Dritten (a) keinen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf verarbeitete Daten und (b) keine für die Sicherung der verarbeiteten Daten verwendete Verschlüsselungsschlüssel für die Plattform bereitstellt, oder solchen Dritten (c) die Möglichkeit einräumt, eine solche Verschlüsselung zu umgehen.

Weitere Informationen zur Verschlüsselung finden Sie in der vorhergehenden Frage.

Wenn ein Kunde eine eigene Verschlüsselung verwendet resp. hinzufügt, ist bezüglich der Verwaltung von Verschlüsselungsschlüsseln folgendes zu beachten: Verschlüsselung und Authentifizierung verbessern die Sicherheit nicht, wenn die Schlüssel selbst nicht gut geschützt sind. Es wird allgemein als eine kritische IT-Sicherheitsaufgabe angesehen, die Lebenszyklen von Schlüsseln zu verwalten, da eine ordnungsgemäße Schlüsselverwaltung wichtig ist, um hohe Sicherheit, hohe Zuverlässigkeit und geringen Overhead zu gewährleisten.

### a. Bring-Your-Own-Key/Hold-Your-Own-Key (BYOK/HYOK)

Azure Key Vault<sup>57</sup> ist ein Cloud-Service für die sichere Speicherung und den Zugriff auf Geheimnisse. Ein Geheimnis können dabei alle Informationen sein, auf welche Kunden den Zugriff streng kontrollieren möchten, wie z.B. API-Schlüssel, Passwörter, Zertifikate oder kryptografische Schlüssel. Dies ermöglicht Organisationen jeder Grösse, ihre eigenen Schlüssel mit extremer Sicherheit zu speichern und zu verwenden - in Übereinstimmung mit den Zugriffsrichtlinien des Tresors -, da auf branchenerprobte, FIPS-konforme Hardware-Sicherheitsmodule (HSMs) verschiedener HSM-Anbieter<sup>58</sup> gesetzt wird. Die BYOK-Fähigkeit ermöglicht es diesen Unternehmen, ihren On-Premises-Schlüssel zu generieren und zu importieren und die Nutzungsrechte für die Verwendung an eine wachsenden Anzahl von Microsoft Cloud-Diensten (wie Microsoft 365 und verschiedene Azure-Dienste) zu delegieren, welche die Integration mit Azure Key Vault für die dientseitige Verschlüsselung, die client-seitige Verschlüsselung und/oder die Inhaltsverschlüsselung zum Schutz ihrer Daten unterstützen.

Die Lösung ist so konzipiert, dass Microsoft die Kundenschlüssel nicht sehen oder extrahieren kann. Eine genauere Beschreibung, wie der Einsatz von Azure Key Vault zu planen und zu implementieren ist, findet sich hier: <https://aka.ms/azurekeyvaultplanning>

Als relativ neuen Dienst bietet Microsoft auch die sogenannte «Double Key Encryption» (<https://docs.microsoft.com/de-ch/microsoft-365/compliance/double-key-encryption?view=o365-worldwide>) an, bei der Microsoft den einen Schlüssel in Microsoft Azure speichert und der Kunde den anderen Schlüssel hält. Der Kunde behält mit dem Dienst «Double Key Encryption» die volle Kontrolle über einen der beiden Kundenschlüssel. Damit kann der Schutz mit dem Azure Information Protection Unified Labeling Client auf Ihre hochsensiblen Inhalte angewendet werden.

Bitte beachten Sie:

BYOK/HYOK-Lösungen (wie z.B. Double Key Encryption) sind nur für die sensibelsten Daten gedacht, die den strengsten Schutzanforderungen unterliegen. Double Key Encryption ist darum nicht für alle Daten gedacht, weil es einige gewichtige Konsequenzen sowohl in Bezug auf Kosten, Komplexität, neue Sicherheitsrisiken (möglicher Verlust der Verfügbarkeit von Daten) und nicht zuletzt auf gelegentliche funktionale Einschränkungen nach sich zieht. Generell sollten Kunden Double Key Encryption nur zum Schutz eines kleinen Teils der gesamten Daten einsetzen. Vor dem Einsatz von Double Key Encryption oder einer anderen BYOK/HYOK-Lösung sollte eine Due Diligence zur Identifizierung der richtigen Daten für die Anwendung solcher Lösungen durchgeführt werden. In einigen Fällen sollten die Datenverantwortlichen den Anwendungsbereich einschränken und für die meisten Daten andere Lösungen verwenden - Lösungen wie Microsoft Information Protection mit Microsoft-managed Keys oder BYOK. Diese Lösungen sind höchstwahrscheinlich ausreichend für Dokumente/Daten, die nicht einem erweiterten Schutz oder allenfalls erweiterten regulatorischen Anforderungen unterworfen sind.

Im Folgenden sind Dienste aufgeführt, die mit Double Key Encryption verschlüsselten Inhalten nicht vollständig genutzt werden können:

- Transportregeln wie Anti-Malware und Spam, die einen Einblick in angehängte Dokumente erfordern.
- Microsoft Delve und MyAnalytics.
- eDiscovery.
- Inhaltssuche und Indexierung.
- Office Web Apps einschliesslich Co-Authoring-Funktionalität.

Alle externen Anwendungen oder Dienste, die nicht mit Double Key Encryption (unter Verwendung von Microsoft Information Protection) integriert sind, können keine Aktionen mit den verschlüsselten Daten durchführen.

Für eine schnelle Einführung in viele dieser Themen stehen auch Videos zur Verfügung, z.B.:

57 <https://azure.microsoft.com/de-de/services/key-vault/>

58 <https://docs.microsoft.com/de-ch/azure/key-vault/keys/hsm-protected-keys>

M365 Double Key Encryption:  
<https://www.youtube.com/watch?v=0d-A4OYxaEA&t=2s>

MyAnalytics: <https://www.youtube.com/watch?v=43i-lXo4wN8>

## 17. Welche Sicherheits- und Datenschutzprüfungen unternimmt Microsoft in Bezug auf eigene Mitarbeiter und die Mitarbeiter von Subunternehmen?

Für einige Core Onlinedienste in Office 365 und Azure unterliegen Mitarbeiter (einschliesslich Mitarbeiter von Subunternehmen) mit potenziellem Zugriff auf Kundendaten einer Hintergrundüberprüfung (soweit dies nach geltendem Recht zulässig ist) und müssen eine Sicherheitsschulung absolvieren.

Die Hintergrundüberprüfung wird in jedem Fall durchgeführt bevor es (in den seltenen Fällen) überhaupt möglich wird, dem Mitarbeiter potenziell die Erlaubnis zu erteilen, auf Kundendaten zuzugreifen. Strafrechtlich relevante Fälle von Betrug, Veruntreuung, Geldwäsche oder berufsbegrenzter Offenlegung unwahrer Informationen, Fälschung oder Unterschlagung können einen Kandidaten von der Beschäftigung ausschliessen oder zur Kündigung des Arbeitsverhältnisses führen.

Siehe auch die CSA Cloud Control Matrix<sup>59</sup>, Seite 40-46 «Human Resources: Controls» und weitere Details im «Microsoft Provider Security and Privacy Assurance Program»: <https://aka.ms/mssspa>

## 18. Wie handhabt Microsoft das Identitäts- und Zugriffsmanagement?

Alle Sicherheitsmaßnahmen sind Teil des Microsoft Control Kit, das in den Berichten SSAE 18 SOC 1 Typ II und SSAE 18 SOC 2 Typ II geprüft wurde.

Microsoft verpflichtet sich im DPA<sup>60</sup> zu mehreren Kontrollen, die gemäss dem Standard ISO/IEC 27002: 2013 «Information Technology - Security Techniques - Code of Practice for Information Security Controls» erforderlich sind, und hat diese auch vollständig implementiert.

Nachfolgend findet sich eine Übersicht (eine detailliertere Beschreibung der Kontrollen finden sich auch in den CSA Cloud Control Matrices<sup>61</sup>):

### Zugriffsberechtigung

- Microsoft pflegt und aktualisiert eine Liste von Mitarbeitern, die zum Zugriff auf Microsoft-Systeme berechtigt sind, die Kundendaten enthalten.
- Microsoft deaktiviert Authentifizierungsmittel, die für einen Zeitraum von maximal sechs Monaten nicht verwendet wurden.
- Microsoft identifiziert Mitarbeiter, die autorisierten Zugriff auf Daten und Ressourcen gewähren, ändern oder aufheben können.
- Microsoft stellt sicher, dass, wenn mehr als eine Person Zugriff auf Systeme hat, die Kundendaten enthalten, diese über getrennte Identifizierungen / Anmeldungen verfügen.
- Least Privilege: Technisches Support-Personal darf nur dann auf Kundendaten zugreifen, wenn dies unbedingt erforderlich ist und vorbehaltlich des definierten und geprüften Lockbox-Verfahrens.
- Microsoft schränkt den Zugriff auf Kundendaten auf diejenigen Personen ein, die diesen Zugriff zur Erfüllung ihrer Arbeitsaufgabe benötigen.

Azure Active Directory<sup>62</sup> ermöglicht zudem Kunden, den Zugriff auf ihre Cloud-Instanzen selber zu verwalten. Darüber hinaus bieten Multi-Faktor-Authentifizierung<sup>63</sup> und Zugriffsüberwachungsdienste<sup>64</sup> erhöhte Sicherheit.

Lesen Sie weitere hilfreiche Tipps zum Thema Identity und Access Management unter: <https://aka.ms/MScloudidam>

59 <https://aka.ms/csamatrixazure> oder <https://aka.ms/csamatrixo365>

60 FN 16

61 <https://aka.ms/csamatrixazure> und <https://aka.ms/csamatrixo365>

62 <https://docs.microsoft.com/de-ch/azure/active-directory/>

63 <https://docs.microsoft.com/de-ch/azure/active-directory/authentication/concept-mfa-howitworks>

64 <https://docs.microsoft.com/de-ch/azure/active-directory/reports-monitoring/overview-reports>

## 19. Wie geht Microsoft mit der Separierung von Kundendaten in einer Multi-Tenant-Umgebung um?

Microsoft isoliert in allen Onlinediensten Kundendaten logisch von anderen Daten, die Microsoft speichert. Die Datenspeicherung und -verarbeitung für jeden Mandanten ist in eine «Azure Active Directory»-Struktur unterteilt, die die einzelnen Kunden durch Sicherheitsgrenzen («Silos») isoliert. Die Silos schützen die Daten des Kunden davor, dass diese nicht von anderen Kunden auf der Plattform abgerufen oder kompromittiert werden können.

Für eine Erklärung des Isolationsansatzes in Microsoft Azure siehe: <https://docs.microsoft.com/de-ch/azure/security/fundamentals/isolation-choices>

Für die Isolierung innerhalb von Microsoft 365 siehe: <https://docs.microsoft.com/de-ch/microsoft-365/enterprise/microsoft-365-tenant-isolation-overview?view=o365-worldwide>

Siehe zudem CSA CCM23-Kontrolle «AAC-03.1», «IVS-08.3», «IVS-09.4».

## 20. Wie werden Anfragen von Behörden nach Datenzugriff oder Datenherausgabe behandelt?

Microsoft arbeitet seit Jahren daran, die öffentliche Sicherheit zu fördern, während wir sicherstellen, dass die Menschen der Technologie vertrauen können. Wir hoffen, dass unsere Beiträge zu modernen Gesetzen führen können, die für alle funktionieren; siehe: <https://aka.ms/datalaw>.

Wir sind der Überzeugung, dass Kunden unsere internen Richtlinien für die Beantwortung von Regierungsanfragen nach ihren Daten kennen sollen. Diese Transparenz hilft auch den politischen Entscheidungsträgern bei der Arbeit an der Modernisierung von Gesetzen, die unsere Kunden betreffen.

Microsoft ist überzeugt, dass Kunden das Recht haben sollen, durch ihre eigenen Gesetze geschützt zu werden. Darüber hinaus glaubt Microsoft, dass die formulierten Prinzipien universelle Rechte und grundlegende Mindestanforderungen darstellen, die den Zugriff von Strafverfolgungsbehörden auf Daten in unserem modernen Zeitalter regeln sollten. Die Anwendung dieser Prinzipien kann von Land zu Land variieren, aber die zugrundeliegenden Prinzipien von Kontrolle und Verhältnismässigkeit, Verantwortlichkeit und Transparenz bleiben bei unserer globalen Tätigkeit bestehen.

Microsoft verfolgt einen prinzipienfesten und strengen Ansatz im Umgang mit staatlichen Anfragen nach Zugriff auf Kundendaten, die sich im Gewahrsam von Microsoft befinden. Die wichtigsten Richtlinien, an die wir uns bei allen unseren Diensten halten, sind:

- Microsoft gewährt keiner Regierung direkten und ungehinderten Zugang zu den Daten unserer Kunden, und wir geben keiner Regierung unsere Verschlüsselungsschlüssel oder die Möglichkeit, unsere 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 Abonnenteninformationen 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.

Der Prozess wird hier im Detail beschrieben: <https://aka.ms/MSLERH>

Ein Teil von Microsofts Arbeit in Bezug auf Regierungsanfragen beinhaltet die Veröffentlichung von «Law Enforcement Request Reports» alle sechs Monate, um Transparenz über den Umfang und die Art dieser Vorfälle zu gewährleisten. Die Berichte sind hier zu finden: <https://aka.ms/MSLERR> und können zur Unterstützung bei der Durchführung von Risikobewertungen beim Kunden verwendet werden.

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.

Wie die Reports und die zugrundeliegenden Anforderungsberichte zeigen, erhält Microsoft weltweit pro Halbjahr nur eine Handvoll gerichtliche Aufforderungen von Strafverfolgungsbehörden in den USA bezüglich kommerzieller Unternehmenskunden, die mehr als 50 «Seats» für eines unserer kommerziellen Cloud-Angebote erworben haben, welche zur Offenlegung von Inhaltsdaten führte, die sich auf Nicht-US-Unternehmenskunden bezogen und deren Daten ausserhalb der USA gespeichert waren.

- Bei der geschätzten Anzahl von Unternehmenskonten in den Microsoft Online Services wird aus den obigen Zahlen 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, bei etwa 1 zu der Anzahl der Kunden liegt, die insgesamt die Microsoft Onlinedienste nutzen.

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 von Anfragen von Strafverfolgungsbehörden aus Drittländern absolut minimal ist.

Zu beachten ist weiter, dass der zahlenmässige Unterschied zwischen Anfragen für Verbraucherkonten und Unternehmenskonten auch die unterschiedlichen formellen Richtlinien<sup>65</sup> der Abteilung für Computerkriminalität und geistiges Eigentum des US-Justizministeriums wider spiegelt, 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. Aus den Richtlinien:

*«(...) Prosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation. (...) Working with counsel and the enterprise's information technology staff, law enforcement can identify and seek disclosure of relevant information. (...) If law enforcement has developed reasons to believe that the enterprise will be unwilling to comply or if the enterprise itself is principally devoted to criminal conduct, seeking disclosure directly from the cloud provider may be the only practical option. (...) Therefore, for any large enterprise, especially one held to high professional standards, it would be difficult for law enforcement to argue [(MSFT): before an independent U.S. judge] that specific facts exist that notification would compromise the investigation.»*

Im Schems II-Urteil werden gewisse US-Überwachungsgesetze genannt, welche Grund für die Einstufung der USA als unsicheres Drittland bieten sollen. Obschon...

- Microsoft eine lange Tradition sowohl der Anfechtung von nachrichtendienstlichen Anfragen<sup>66</sup> als auch der Prozesse rund um solche Anfragen<sup>67</sup> hat,

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

66 <https://aka.ms/MSSecrecyOrdersHistory>

67 <https://aka.ms/MSSecrecyOrders2021>

- Microsoft versichern kann, dass keine Drittpartei ungehinderten Zugang weder zu Daten noch zu Verschlüsselungsschlüsseln hat (und auch nie hatte),
- Microsoft die Schutzmechanismen in der Microsoft Cloud-Infrastruktur stetig verbessert<sup>68</sup>,
- Microsoft Reformen<sup>69</sup> der Überwachungspraktiken fordert, und nicht zuletzt, dass
- Microsoft dafür kämpft<sup>70</sup>, die bestmögliche Transparenz über den Umfang und die Ergebnisse solcher Anfragen bieten zu können...

... ist eine vollständige Transparenz aus Gründen der nationalen Sicherheit derzeit rechtlich nicht möglich ist. Die Berichte, die Microsoft auf der Grundlage der US-Überwachungsgesetze zu diesen Anfragen veröffentlichen darf, liefern jedoch genügend Information, damit Unternehmenskunden das Risiko einschätzen können, ob ihre Daten Ziel von nachrichtendienstlichen Anfragen sein könnten. Wie bei den Law Enforcement Requests ist die Gesamtwahrscheinlichkeit (und damit das Risiko) eindeutig auf einem absoluten Minimum, und zwar in einem Masse, das die meisten Sicherheitsexperten als akzeptabel, wenn nicht sogar als vernachlässigbar ansehen würden. Die Berichte, die Microsoft rechtmäßig veröffentlichen darf, sind hier zu finden: <https://aka.ms/MSLERNSO>

Beachten Sie, dass die Prozesse und vertraglichen Verpflichtungen von Microsoft in Bezug auf die Beantwortung von Regierungsanfragen auch für Anfragen gelten, die die nationale Sicherheit betreffen. Microsoft interagiert täglich mit Kunden und Regierungen auf der ganzen Welt und gestaltet so den internationalen Rechtsrahmen für diese kritischen Themen mit. Als Leitfaden für diese Arbeit hat Microsoft sechs Prinzipien veröffentlicht:

#### «SIX PRINCIPLES FOR INTERNATIONAL AGREEMENTS GOVERNING

LAW ENFORCEMENT ACCESS TO DATA»:

<https://aka.ms/MS6dataaccessPrinciples>

68 <https://aka.ms/MSProtectingDataFromGovernments>

69 <https://aka.ms/MSReformGovernmentSurveillance>

70 <https://aka.ms/MSSecrecyOrders>



Microsoft verpflichtet sich vertraglich zur Verantwortung für diesen Umgang, wie er im DPA<sup>71</sup> unter «Offenlegung verarbeiteter Daten», Seite 6, ausdrücklich definiert ist. Zudem wurde nach dem Schrems-II-Urteil eine weitere Verpflichtung, jede Anfrage Dritter nach Kundendaten anzufechten, ins DPA (Anhang C – Nachtrag zu zusätzlichen Schutzmassnahmen) aufgenommen, der für die gesamte Unternehmensnutzung der Microsoft Onlinedienste gilt.

#### **21. Werden Subunternehmer eingesetzt? Und wenn ja, unter welchen Bedingungen und wofür?**

Das DPA<sup>72</sup> beschreibt unter «Hinweise und Kontrolle beim Einsatz von Unterauftragsverarbeitern» wie Microsoft mit Unterauftragnehmern umgeht und Kunden über Änderungen im Portfolio der Unterauftragnehmer etc. benachrichtigt.

Im Services Trust Center wird eine Liste geführt über die von Unterauftragnehmern erbrachten Dienste, des Standorts ihres Hauptsitzes und des Umfangs und der Bedingungen, unter denen sie auf Kundendaten zugreifen können: <http://aka.ms/mscloudsubprocessors>.

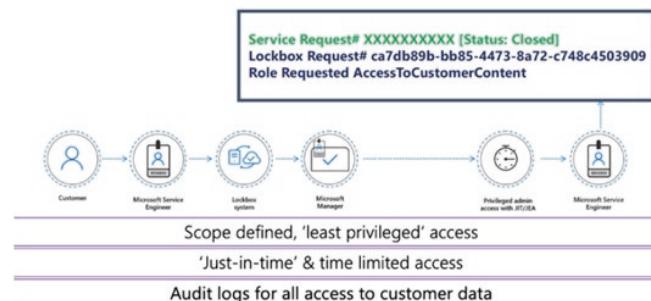
Die genauen Bedingungen für den Einsatz von Subunternehmern und den Datenzugriff durch diese finden Sie im DPA<sup>73</sup> und eine kurze Leseanleitung finden Sie hier: <https://aka.ms/msclouddataaccess>, für Azure hier: <https://aka.ms/AzureDataAccess> und für O365 hier: <https://aka.ms/o365dataaccess>

Darin wird beschrieben, welche Anforderungen Microsoft an den Unterauftragnehmer stellt (einschliesslich der Untergruppe, die als Unterdatenbearbeiter gilt) und dass Microsoft dafür verantwortlich ist, dass die Unterauftragnehmer alle Anforderungen gemäss DPA erfüllen.

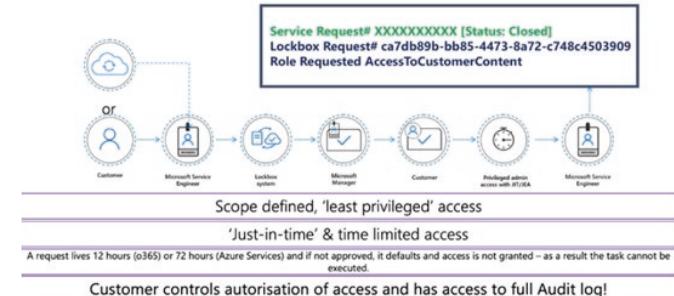
Weder Microsoft noch Unterauftragnehmer haben ständigen administrativen Zugriff auf Kundendaten oder Kundenlösungen. Microsoft Cloud arbeitet mit «Zero standing ADMIN» auch bekannt als «Least Privilege», bei dem der administrative Zugriff durch ein Authentifizierungsverfahren (genannt «Lock-box») kontrolliert wird, z.B. im Fall von Kunden, die Microsoft mit einer Supportaufgabe beauftragen, die dem mit dem Supportfall betrauten Mitarbeiter Privilegien einräumen (welche einen Zugriff auf Kundendaten im Einzelfall ermöglichen könnten). Die Zuteilung dieses 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».

Im Folgenden werden die beiden Verfahren dargestellt:

#### **Microsoft Lockbox approval workflow**

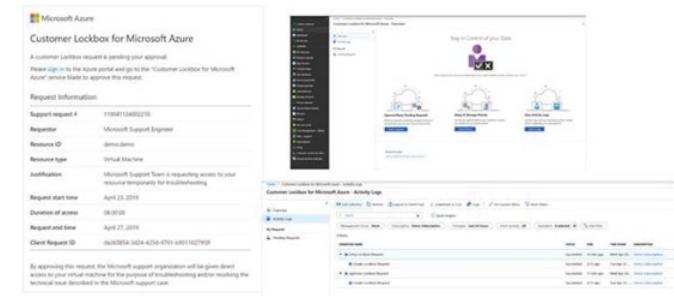


#### **Customer Lockbox approval workflow**



Lockbox, erweiterbar um die Endfreigabe durch den Kunden:

Der Kunde hat die freie Wahl, die Aufgabe wie beschrieben erledigen zu lassen:



Lesen Sie mehr über die «Customer Lockbox»-Steuerung unter diesen Links:

71 FN 16

72 FN 16

73 FN 16

<https://aka.ms/msazurelockbox> und  
<https://aka.ms/o365CustomerLockbox>

**22. In welchem Umfang werden Daten in Länder ausserhalb der EU/EWR übertragen? Welche rechtlichen Kontrollen, Sicherheits- und Datenschutzmassnahmen stehen dem Kunden zur Verfügung, um eine Risikobewertung durchzuführen und Übertragungen zu dokumentieren?**

Das DPA<sup>74</sup> definiert unter «Datenübermittlungen und Speicherstelle» in welchen Fällen eine Übertragung (im rechtlichen Sinne) stattfinden kann.

Der Standardbetrieb der Microsoft Core Onlinedienste<sup>75</sup> erfordert in der Regel keinen Zugriff auf oder die Einsicht in Kundendaten. Die internen Standardrichtlinien von Microsoft sehen vor, dass, wenn ein solcher Zugriff gewährt werden soll, dieser dem oben in Frage 21 beschriebenen «Lockbox»-Prozess folgt. Und wenn der Kunde die Funktion «Customer Lockbox» implementiert und konfiguriert hat, erfordert dies zusätzlich das Einverständnis des Kunden. Unabhängig davon, ob die «Customer Lockbox» hinzugefügt wurde oder nicht, werden alle Fälle von Zugriffen in den regulären Audit-Protokollen des Kunden dokumentiert und können so in die Compliance-Dokumentation aufgenommen werden.

Eine detaillierte Beschreibung, wie der Datenzugriff in der Microsoft Cloud gehandhabt wird findet sich hier: <https://aka.ms/azuredataaccess> & <https://aka.ms/o365dataaccess>

**23. Gibt es Hilfestellungen für die Beschaffung, Bereitstellung, Migration und zur Sicherstellung der Compliance von Onlinediensten?**

**a. Use Cases von bestehenden Kunden**

Millionen von Kunden in allen Branchen auf der ganzen Welt nutzen heute die vielen verfügbaren Microsoft-Cloud-Dienste - zur Inspiration finden sich online verschiedene Fallbeschreibungen: <https://aka.ms/msazurercases>

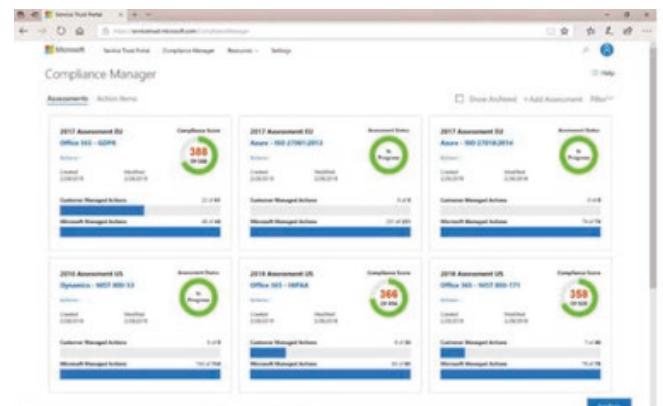
Das Portal <https://azure.microsoft.com/en-us/industries/government/> bietet Zugang zu einer Fülle von Informationen über Lösungen, die speziell auf ausgewählte Branchen ausgerichtet sind (z.B. öffentlicher Sektor<sup>76</sup>), technische und Compliance-Dokumentation, Entwickler-Tools, Schulungen<sup>77</sup> sowohl für Entwickler als auch für Betreiber und Anwender usw. Ähnliche Informationen sind auch für Microsoft 365 und Dynamics 365 verfügbar.

**b. Cloud-Kostenanalyse (TCO):**

Das «Microsoft Configuration and Pricing Portal»<sup>78</sup> ermöglicht es Kunden, die Kosten für Inbetriebnahme und den Betrieb aller Cloud Services abzuschätzen und zu prognostizieren.

**c. Compliance Aufgaben**

Der Microsoft Compliance Manager<sup>79</sup> vereinfacht die Aufgabe, Risikobewertungen der Nutzung von Microsoft Cloud-Diensten durchzuführen. Mit dem Compliance Manager können Unternehmen ihre Compliance-Aktivitäten von der Implementierung bis zum Reporting verwalten und eine Liste geeigneter technischer und organisatorischer Massnahmen führen. Der Compliance-Manager verlinkt auch auf den gesamten Katalog der Microsoft Cloud Standard-Zertifizierungen und Audit-Berichte, bis hin zu jeder einzelnen Sicherheitsprüfung / Massnahme und gibt so dem Kunden einen Überblick über die Kontrollen, die Microsoft als Datenbearbeiterin in Übereinstimmung mit der aktuellen Best Practice oder dem ausgewählten Standard (ISO27001, PCI, FedRAMP, etc.) implementiert hat.



74 FN 16

75 FN 16

76 <https://azure.microsoft.com/da-dk/industries/government/>

77 <https://docs.microsoft.com/da-dk/learn/azure/>

78 <https://aka.ms/MSCloudTCO>

79 <https://aka.ms/mscompliancemanager>

#### d. Optimierung der Cloud-Implementierung

Azure Advisor<sup>80</sup> ist ein persönlicher Cloud-Berater, der Kunden hilft, mit der Befolgung von Best Practices Azure-Implementierungen zu optimieren. Er analysiert die Ressourcenkonfiguration und -nutzung und empfiehlt dann Lösungen, die zur Verbesserung von Kosteneffizienz, Leistung, Hochverfügbarkeit und Gesamtsicherheit beitragen können.

##### You have free Azure Advisor recommendations!

Azure Advisor is a free offering that analyzes your Azure usage and provides recommendations on how you can save money, improve performance, be more secure, and improve reliability of the solutions you already have running in Azure. [Learn more](#)



Über den «Secure Score»<sup>82</sup> bietet das Dashboard einen Überblick über die Sicherheit der Cloud-Bereitstellung und Best-Practice-Empfehlungen für die weitere Priorisierung (siehe Frage 10).

Für Azure zeigt das Dashboard z.B. häufige Fehlkonfigurationen für Azure Infrastructure as a Service (IaaS)- und Platform as a Service (PaaS)-Ressourcen auf, wie z.B.: Versäumnisse bei der Implementierung von System-Updates auf virtuellen Maschinen (VMs).

- Unnötige Exposition gegenüber dem Internet durch Public Facing-Endpunkte.
- Nicht verschlüsselte Daten bei der Übertragung oder Speicherung.

Für Microsoft 365 kann die Befolgung der Secure Score-Empfehlungen Unternehmen vor Bedrohungen schützen. Über ein zentrales Dashboard im Microsoft 365-Sicherheitscenter können Organisationen an der Sicherheit ihrer Microsoft 365-Identitäten, Apps und Geräte arbeiten. Secure Score hilft Organisationen:

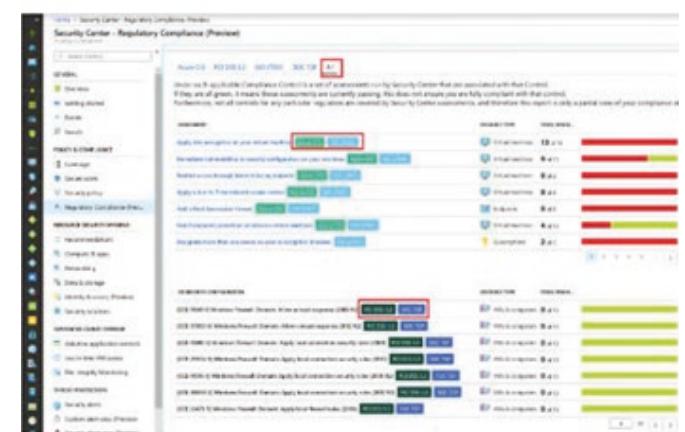
Berichte über den aktuellen Stand der Sicherheitslage der Organisation zu erstellen.

Ihre Sicherheitslage zu verbessern, indem sie Erkennbarkeit, Transparenz, Orientierung und Kontrolle bieten.

Vergleiche mit Benchmarks und Festlegung von Key Performance Indicators (KPIs) vorzunehmen.

Organisationen erhalten so Zugriff auf robuste Visualisierungen von Metriken und Trends, Integrationen mit anderen Microsoft-Produkten, Vergleiche des Scores von vergleichbaren Organisationen und vieles mehr. Der Score kann auch erfassen, wenn Lösungen von Drittanbietern die empfohlenen Massnahmen umgesetzt haben.

#### f. Regulatorische Compliance



Das M365 Compliance Center<sup>83</sup> bietet detaillierte Einblicke in die Gesamt-Compliance<sup>84</sup>, basierend auf laufenden Bewertungen der Implementierung. Das Security Center analysiert Risikofaktoren in einer (potenziell auch hybriden) Cloud-Umgebung gemäss Best Security Practices. Diese Bewertungen sind mit der Compliance-Überwachung aus einer Reihe von unterstützten Standards verknüpft. Das Compliance-Dashboard zeigt den Status aller Bewertungen in Bezug auf einen bestimmten Standard oder eine bestimmte Vorschrift an. Wenn die Empfehlungen<sup>85</sup> und Risikofaktoren in der Konfiguration reduziert werden, wird die Gesamt-Compliance verbessert.

80 <https://aka.ms/msazureadvisor>

81 <https://aka.ms/AzureSecurityCenterDoc>

82 <https://aka.ms/m365SecureScore> und <https://aka.ms/AzureSecureScore>

83 <https://aka.ms/m365ComplianceCenter>

84 <https://aka.ms/MSComplianceDashboard>

85 <https://aka.ms/azuresccd>

Das Security Center kann auch die Verwaltung von Sicherheitseinstellungen und den Schutz vor Bedrohungen in Implementierungen mit anderen Cloud-Anbietern und VMs in der lokalen Umgebung integrieren sowie Server-Agenten für die Ausführung in der lokalen/vor-Ort-Umgebung vorbereiten. Es kann auch eine Verbindung zu bestehenden Tools und Prozessen herstellen, wie z.B. Security Information and Incident Management (SIEM) oder Sicherheitslösungen von Partnern integrieren.

Azure Sentinel<sup>86</sup> erweitert die SIEM-Domäne um die Fähigkeiten eines Online-Dienstes. Darüber hinaus enthält Sentinel Funktionen zur automatisierten Sicherheitsorchestrierung, um intelligente Sicherheitsanalysen und Bedrohungssichten im gesamten Unternehmen bereitzustellen und eine einzige Lösung für die Erkennung von Alarms, die Sichtbarkeit von Bedrohungen, die proaktive Suche und die Reaktion auf Bedrohungen zu bieten.

Sammeln von Daten über alle Benutzer, Geräte, Anwendungen und Infrastrukturen, sowohl vor Ort als auch in mehreren Clouds.

Erkennen von bisher unentdeckten Bedrohungen und Minimierung sog. «False Positives» mit Hilfe von Microsoft Analytics und Threat Intelligence.

Untersuchung von Bedrohungen mit künstlicher Intelligenz und Suchen nach verdächtigen Aktivitäten, wobei auf die jahrelange Arbeit von Microsoft im Bereich Cybersicherheit zurückgegriffen werden kann.

Schnelle Reaktion auf Vorfälle mit integrierter Orchestrierung und Automatisierung von allgemeinen Aufgaben.

#### g. Sicherstellung einer optimalen Implementierung und Konfiguration

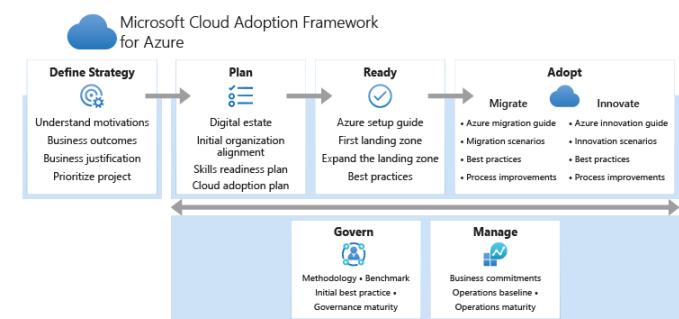


Azure Blueprints<sup>87</sup> und Azure Policy Blueprints<sup>88</sup> sind Cloud-Ressourcen, die dabei helfen, Cloud-basierte Anwendungen zu erstellen und zu starten, unter Berücksichtigung von Regeln, Richtlinien und Standards, wie sie vom Datenverantwortlichen definiert wurden. Sie beinhalten:

- Branchenspezifische Übersicht und Anleitungen.
- Matrix für Kundenverantwortung.
- Referenzarchitekturen mit Bedrohungsmustern.
- Kontrolle der Implementierungsmatrizen.
- Automatisierung für die Implementierung von Referenzarchitekturen.

Azure Policy ist ein Dienst, mit dem Richtlinien erstellt, zugewiesen und verwaltet werden können. Diese Richtlinien setzen ausgewählte Regeln für die in der Lösung verwendeten Ressourcen durch, damit diese Ressourcen den Unternehmensstandards, Compliance-Anforderungen und Service Level Agreements entsprechen. Azure Policy erfüllt diese Anforderung, indem es die Ressourcen auf die Nichteinhaltung zugewiesener Richtlinien hin überprüft. Zum Beispiel kann eine Richtlinie festlegen, dass nur eine bestimmte SKU-Größe auf virtuellen Maschinen in der Umgebung erlaubt ist. Sobald diese Richtlinie implementiert ist, werden neue und bestehende Ressourcen auf Konformität bewertet, um die Einhaltung / Konformität mit den gewählten Richtlinien und Standards des Unternehmens zu gewährleisten.

#### h. Leitfaden zur Cloud-Anwendung



<sup>86</sup> Service: <https://aka.ms/AzureSentinel> & Beschreibung: <https://aka.ms/MSAzureSentinel>

<sup>87</sup> <https://aka.ms/azureblueprints>

<sup>88</sup> <https://aka.ms/msazurepolicies>

Das Microsoft Cloud Adoption Framework (CAF)<sup>89</sup> ist der einheitliche Microsoft-Leitfaden für die Einführung und Implementierung der Cloud. CAF konsolidiert und teilt Best Practices von Microsoft selbst, Partnern und Kunden. Es bietet eine Reihe von Werkzeugen und Anleitungen, die bei der Gestaltung von Technologie-, Geschäfts- und Ressourcenstrategien helfen und so die gewünschten Geschäftsergebnisse durch die Cloud-Nutzung fördern. Die Anleitungen sind auf eine Reihe von Phasen des Cloud-Implementierungs-Lebenszyklus abgestimmt und gewährleisten einen einfachen Zugriff auf die richtigen Anleitungen zur richtigen Zeit: Strategie, Planung, Vorbereitung, Migration, Entwicklung, Governance und Betrieb.

Der Azure Migration Service<sup>90</sup> hilft bei der Bewertung, Planung, Migration, Optimierung und Verwaltung der Migration in die Cloud-Umgebung. Hier haben Sie Zugang zu allen notwendigen Tools und Ressourcen<sup>91</sup> in Ihrem gewünschten Tempo und ohne unnötige Sorgen.

Für Partner bietet Microsoft ausserdem das Cloud Migration Playbook<sup>92</sup> an, das Hilfestellung und Beratung, Migration von Workloads oder Modernisierung älterer Microsoft Cloud Anwendungen / Lösungen bietet. Ähnliche Leitfäden gibt es für spezifische Lösungsbereiche wie KI, IoT, Operations, Cloud App-Entwicklung etc.

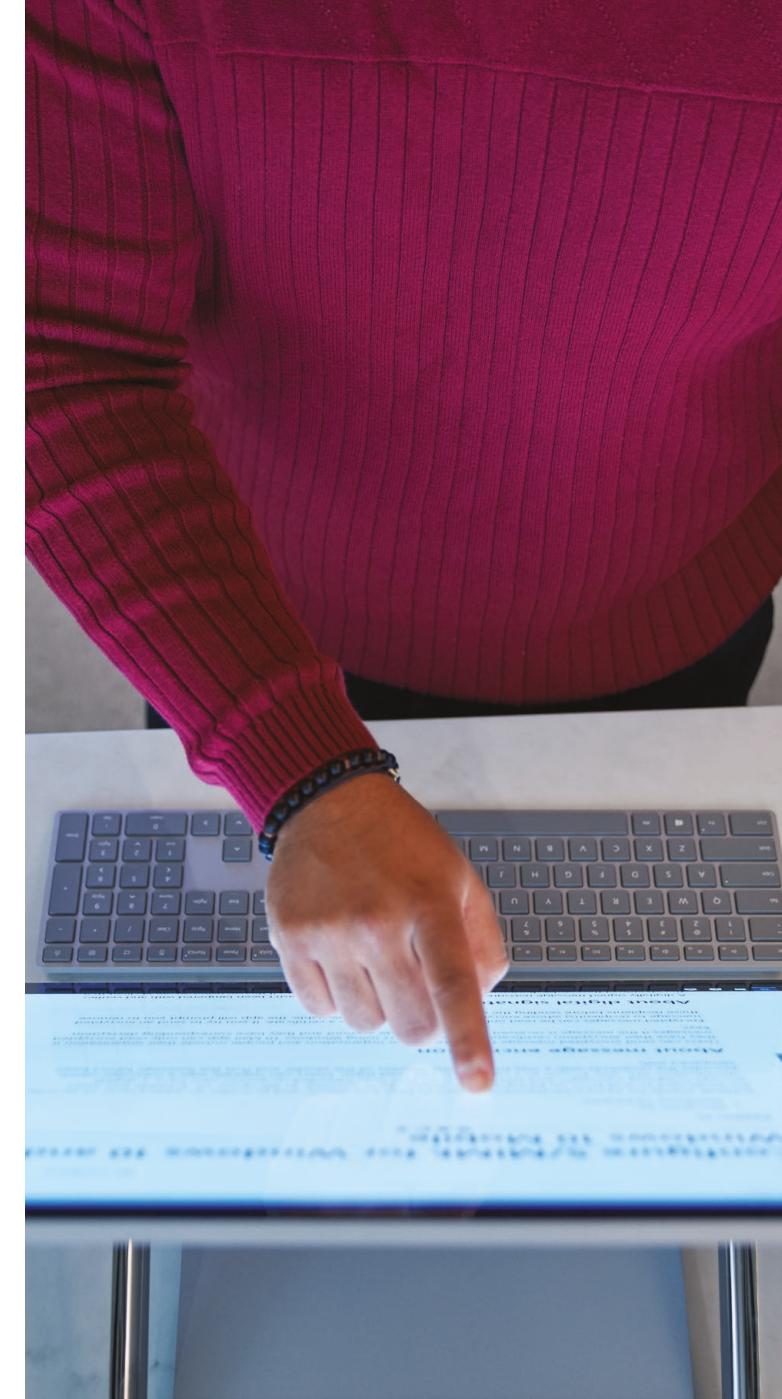
Die oben genannten Funktionen und Lösungen sind für alle Microsoft Cloud-Dienste anwendbar. Für einige Dienste sind zusätzliche Tools verfügbar, die einen Überblick geben und Massnahmen empfehlen, um die Einhaltung von Vorschriften und die allgemeine Sicherheit zu verbessern. Zum Beispiel für die Microsoft 365 Plattform:

Microsoft Secure Score: <https://aka.ms/m365secscore>

Office 365 Security & Compliance Center:  
<https://aka.ms/m365seccmplcenter>

### i. Insider-Risikomanagement

Das Microsoft 365 Insider Risk Management<sup>93</sup> hilft, interne Risiken zu minimieren, indem es Kunden ermöglicht, böswillige und unbeabsichtigte Aktivitäten im eigenen Unternehmen zu erkennen, zu untersuchen und darauf zu reagieren. Mit den Richtlinien für Insider-Risiken können die Arten von Risiken definiert werden, die in der eigenen Organisation erkannt und aufgedeckt werden sollen, einschliesslich der Reaktion auf Fälle und der Eskalation von Fällen an Microsoft Advanced eDiscovery, falls erforderlich. Risikoanalysten im Unternehmen können so rasch geeignete Massnahmen ergreifen, um sicherzustellen, dass die Benutzer die Compliance-Standards des Unternehmens einhalten.



<sup>89</sup> <https://aka.ms/MScaf>

<sup>90</sup> <https://aka.ms/azuremigrering>

<sup>91</sup> <https://aka.ms/azurermigrationtools>

<sup>92</sup> <https://assets.microsoft.com/en-us/mpn-playbook-cloud-migration.pdf>

<sup>93</sup> <https://aka.ms/M365InsiderRisk>

## IV. ANHANG – DATENSCHUTZRECHTLICHE BESTIMMUNGEN BUND UND KANTONE

ERLÄSSE	AUFRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<p><b>Bund</b> Datenschutzverordnung (DSV) Direktionsverordnung über Informationsicherheit und Datenschutz (IDS) DV</p> <p>Allgemeine Geschäftsbedingungen des Kantons Bern über die Informationsicherheit und den Datenschutz (IDS) bei der Erbringung von Informatikdienstleistungen (AGB IDS)</p>	<p><a href="https://www.legifind.ch/fid/e/10123528/version/191742/die/">https://www.legifind.ch/fid/e/10123528/version/191742/die/</a>  <a href="https://www.legifind.ch/fid/e/10123679/version/132914/de/">https://www.legifind.ch/fid/e/10123679/version/132914/de/</a></p> <p><a href="https://www.kas.ch/be/ch/content/dam/kas/documente/rechtliche-grundlagen/idsv1_1_agb%20ids%20be%20v%20%20%20.pdf">https://www.kas.ch/be/ch/content/dam/kas/documente/rechtliche-grundlagen/idsv1_1_agb%20ids%20be%20v%20%20%20.pdf</a></p>		<p><b>Art. 10a DSG Datenbearbeitung durch Dritte</b> 1 Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. 2 Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet. 3 Dritte können dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.</p> <p><b>Art. 7 DSG Datensicherheit</b> 1 Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. 2 Der Bundesrat erlässt nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit.</p> <p><b>Art. 8 VDSG Technische und organisatorische Massnahmen – Allgemeine Massnahmen</b> 1 Wer als Vertragspartner Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten, um einen angemessenen Datenschutz zu gewährleisten. Insbesondere schützt er die Systeme gegen folgende Risiken: a. unbefugte oder zufällige Vernichtung; b. zufälligen Verlust; c. technische Fehler; d. Fälschung, Diebstahl oder widerrechtliche Verwendung; e. unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. 2 Die technischen und organisatorischen Massnahmen müssen angemessen sein. Insbesondere tragen sie folgenden Kriterien Rechnung: a. Zweck der Datenbearbeitung; b. Art und Umfang der Datenbearbeitung; c. Einschätzung der möglichen Risiken für die betroffenen Personen; d. gegenwärtiger Stand der Technik. 3 Diese Massnahmen sind periodisch zu überprüfen.</p> <p><b>Art. 9 VDSG Technische und organisatorische Massnahmen – Besondere Massnahmen</b> 1 Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden: a. Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren; b. Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen; c. Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können; d. Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können; e. Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern; f. Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern; g. Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen; h. Eingabekontrolle: in Automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden. 2 Die Datensammlungen sind so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können.</p>	<p><b>Art. 6 DSG Grenzüberschreitende Bekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Personendaten der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b. die betroffene Person im Einzelfall eingewilligt hat; c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt; d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegender öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; g. die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten. 3 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Beauftragte, Art. 26) muss über die Garantien nach Absatz 2 Buchstabe a und die Datenschutzregeln nach Absatz 2 Buchstabe g informiert werden. Der Bundesrat regelt die Einzelheiten dieser Informationspflicht.</p> <p><b>Art. 6 VDSG Informationspflicht</b> 1 Der Inhaber der Datensammlung informiert den Beauftragten vor der Bekanntgabe ins Ausland über die Garantien und Datenschutzregeln nach Artikel 6 Absatz 2 Buchstaben a und g DSG. Ist die vorgängige Information nicht möglich, so hat sie unmittelbar nach der Bekanntgabe zu erfolgen. 2 Wurde der Beauftragte über die Garantien und die Datenschutzregeln informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die: a. unter denselben Garantien erfolgen, soweit die Kategorien der Empfänger, der Zweck der Bearbeitung und die Datengattungen im Wesentlichen unverändert bleiben; oder b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfinden, soweit die Datenschutzregeln weiterhin einen angemessenen Schutz gewährleisten. 3 Die Informationspflicht gilt ebenfalls als erfüllt, wenn Daten gestützt auf Musterverträge oder Standardvertragsklauseln übermittelt werden, die vom Beauftragten erstellt oder anerkannt wurden, und der Beauftragte vom Inhaber der Datensammlung in allgemeiner Form über die Verwendung dieser Musterverträge oder Standardvertragsklauseln informiert wurde. Der Beauftragte veröffentlicht eine Liste der von ihm erstellten oder anerkannten Musterverträge und Standardvertragsklauseln. 4 Der Inhaber der Datensammlung trifft angemessene Massnahmen um sicherzustellen, dass der Empfänger die Garantien und die Datenschutzregeln beachtet.</p> <p><b>Art. 7 VDSG Liste der Staaten mit angemessener Datenschutzgesetzgebung</b> Der Beauftragte veröffentlicht eine Liste der Staaten, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet.</p>	<p><b>Art. 320 StGB Verletzung des Amtsgeheimnisses</b> 1 Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar. 2. Der Täter ist nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde geoffenbart hat.</p>

ERLASSE	AUFTRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Revidiertes Datenschutzgesetz</b> Bundesgesetz über den Datenschutz; Revision; Text gemäß Schlussabstimmung vom 25. September 2020 (revDSG)	<p><b>Art. 9 revDSG Bearbeitung durch Auftragsbearbeiter</b></p> <p>1 Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:</p> <ul style="list-style-type: none"> <li>a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun durfte; und</li> <li>b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.</li> </ul> <p>2 Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.</p> <p>3 Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.</p> <p>4 Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.</p>		<b>Art. 8 revDSG Datensicherheit</b>	<p>1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Maßnahmen eine dem Risiko angemessene Datensicherheit.</p> <p>2 Die Maßnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.</p> <p>3 Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.</p>	<p><b>Art. 16 revDSG – Bekanntgabe von Personendaten ins Ausland – Grundsätze</b></p> <p>1 Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.</p> <p>2 Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:</p> <ul style="list-style-type: none"> <li>a. einen vollkurrechtlichen Vertrag;</li> <li>b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden;</li> <li>c. spezifische Garantien, die das zuständige Bundesamt erarbeitet und dem EDÖB vorgängig mitgeteilt hat;</li> <li>d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder</li> <li>e. verbindliche unternehmensinterne Datenschutzzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden.</li> </ul> <p>3 Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen.</p>

ERLASSE	AUFRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Aargau</b> Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG)	<a href="https://www.legifind.ch/fv/de/tot/1371/de">https://www.legifind.ch/fv/de/tot/1371/de</a> <a href="https://www.legifind.ch/fv/de/tot/934/versions/193648/de">https://www.legifind.ch/fv/de/tot/934/versions/193648/de</a>	<b>§ 18 IDAG Datenbearbeitung im Auftrag</b> 1. Auftragnehmende für die Bearbeitung von Personendaten durch Dritte bearbeiten, stellt es den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicher. Insbesondere dürfen Auftragsdatenbearbeitende Bearbeitungen von Personendaten ohne vorgängige schriftliche Zustimmung des öffentlichen Organs keinen weiteren Auftragnehmenden übertragen. 2. Das öffentliche Organ bleibt für die Einhaltung des Datenschutzes verantwortlich. Die Rechte der Betroffenen sind ihm gegenüber geltend zu machen.	<b>§ 12a VIDAG Datenverarbeitung im Auftrag</b> 1. Auftragnehmende für die Bearbeitung von Personendaten sind vom öffentlichen Organ unter besonderer Berücksichtigung der von jenen getroffenen technischen und organisatorischen Massnahmen sorgfältig auszuwählen. Durch Vertrag oder Auflagen sind festzulegen: (...) g) Kontrollrechte des auftraggebenden öffentlichen Organs und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmenden; h) Mitteilungspflicht des Auftragnehmenden bei Verletzungen der Datensicherheit; i) Weisungsbefugnis des öffentlichen Organs; j) die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmenden gespeicherter Daten. 2. Stellt die Bearbeitung von Personendaten nicht die Hauptpflicht des Auftragnehmenden dar, haben sich die Vereinbarung oder die Auflagen sinngemäss am Inhalt gemäss Abs. 1 zu orientieren.	<b>§ 12 IDAG Datensicherheit</b> 1. Personendaten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. 2. Das verantwortliche öffentliche Organ ist verpflichtet, den Nachweis zu erbringen, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt die Einzelheiten durch Verordnung.  Konkretisierungen in § 4 f. VIDAG.	(ev. analoge Anwendung gewisser Regeln in § 14 Abs. 3 und 4 IDAG in der Praxis)
<b>Appenzell Ausserrhoden</b> Gesetz über den Datenschutz (DSGAR)	<a href="https://www.legifind.ch/fv/de/tot/2310/versions/8398/de">https://www.legifind.ch/fv/de/tot/2310/versions/8398/de</a>	<b>Art. 15 DSGAR Bearbeitung durch Drittpersonen</b> 1 Überträgt das Organ die Bearbeitung von Daten einer Drittperson, so stellt es den Datenschutz durch Auflagen, durch Vereinbarungen oder auf andere Weise sicher.	<b>Art. 16 DSGAR Datensicherheit</b> 1 Wer Daten bearbeitet, sichert sie durch technische und organisatorische Vorkehrungen vor Verlust, Entwendung sowie unbefugter Kenntnisnahme und Bearbeitung.	<b>Art. 13a DSGAR Bekanntgabe ins Ausland</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, nämlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a) hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b) die betroffene Person im Einzelfall eingewilligt hat; c) die Bekanntgabe im Einzelfall für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; d) die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; e) die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	
<b>Appenzell Innerrhoden</b> Datenschutz-, Informations- und Archivgesetz (DIAG)	<a href="https://www.legifind.ch/fv/de/tot/1195/versions/189794/de">https://www.legifind.ch/fv/de/tot/1195/versions/189794/de</a>	<b>Art. 6 DIAG Übertragung an Dritte</b> 1 Das Bearbeiten von Personendaten kann übertragen werden, wenn: a) dafür eine einschneidige abstrakte oder schriftliche verteilende Regelung besteht, b) der Auftrag klar umschrieben ist und c) die Einhaltung der gesetzlichen Vorgaben durch geeignete Massnahmen sicher gestellt ist. 2 Das beauftragende öffentliche Organ bleibt mitverantwortlich. Eine Weiterübertragung ist nur mit seiner schriftlichen Zustimmung möglich.	<b>Art. 9 DIAG Schutz und Verantwortung</b> 1 Personendaten sind durch technische und organisatorische Massnahmen angemessen gegen unbefugtes Bearbeiten zu schützen. 2 Für den Schutz und die Sicherheit von Daten ist das Organ verantwortlich, welches diese bearbeitet oder bearbeiten lässt. 3 Bearbeiten mehrere Organe einen gemeinsamen Datenbestand, trägt innerer Linie der Inhaber oder der Inhaberin des Bestandes die Verantwortung. Jedes Organ bleibt für seinen Bereich verantwortlich.	(ev. analoge Anwendung gewisser Regeln in Art. 16 DIAG (Bekanntgabe ins Ausland an öffentlich Organe) in der Praxis)	

ERLÄSSE	AUFRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Basel-Landschaft</b> Gesetz über die Information und den Datenschutz (IDGBL) Verordnung zum Gesetz über die Information und den Datenschutz (IDVBL) Verordnung über die Informationssicherheit (VISBL)	<a href="https://www.lexfind.ch/fe/tol/3003/versions/19590/de/">https://www.lexfind.ch/fe/tol/3003/versions/19590/de/</a> <a href="https://www.lexfind.ch/fe/tol/2999/versions/192396/de">https://www.lexfind.ch/fe/tol/2999/versions/192396/de</a> <a href="https://www.lexfind.ch/fe/tol/3788/versions/16289/de">https://www.lexfind.ch/fe/tol/3788/versions/16289/de</a>		<b>§ 7 IDGBL Bearbeiten im Auftrag</b> 1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn: a. keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und b. sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun durfte. 2 Das öffentliche Organ bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.	<b>§ 8 IDGBL Informations sicherheit</b> 1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen vor Verlust, Entwendung sowie unrechtmäßiger Bearbeitung und Kenntnisnahme. 2 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik. 3 Der Regierungsrat regelt das Nähere.  Konkretisierungen in § 1ff. IDVBL und VISBL.	<b>§ 21 IDGBL Grenzüberschreitende Bekanntgabe von Personendaten</b> 1 Öffentliche Organe dürfen Personendaten anderen Organen oder Privaten, die nicht der Rechts hoheit eines Staates unterstehen, der dem Europarat übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogene Daten beigetreten ist, nur bekannt geben, wenn: a. die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleistet; b. durch vertragliche Vereinbarungen ein angemessener Schutz garantiert wird; c. dies im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; oder d. im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf. 2 Vorbehalt bleiben die gesetzlichen Bestimmungen über den Austausch und die Weiterverarbeitung von Personendaten im Rahmen des Schengener Informationssystems (SIS).
<b>Basel-Stadt</b> Gesetz über die Information und den Datenschutz (IDGBS) Verordnung über die Information und den Datenschutz (IDVBS)	<a href="https://www.lexfind.ch/fe/tol/32090/versions/187180/de">https://www.lexfind.ch/fe/tol/32090/versions/187180/de</a> <a href="https://www.lexfind.ch/fe/tol/4772/versions/186723/de">https://www.lexfind.ch/fe/tol/4772/versions/186723/de</a>		<b>§ 7 IDGBS Bearbeiten im Auftrag</b> 1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn: a) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und b) sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun durfte. 2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.	<b>§ 8 IDGBS Informations sicherheit</b> 1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen. 2 Die Massnahmen richten sich nach den folgenden Schutzzügen: a) Informationen dürfen nicht unrechtmäßig zur Kenntnis gelangen (Vertraulichkeit); b) Informationen müssen richtig und vollständig sein (Integrität); c) Informationen müssen bei Bedarf vorhanden sein (Zurechenbarkeit); d) Informationsbearbeitungen müssen einer Person zugerechnet werden können (Zurechenbarkeit); e) Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (Nachvollziehbarkeit). 3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik. 4 Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung.	<b>§ 23 IDGBS Grenzüberschreitende Bekanntgabe von Personendaten</b> 1 Öffentliche Organe dürfen Personendaten anderen Organen oder Privaten, die nicht der Rechts hoheit eines Staates oder einer Organisation unterstehen, welche dem Europarat übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogene Daten beigetreten sind, nur bekannt geben, wenn: a) die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleistet oder b) durch vertragliche Vereinbarungen ein angemessener Schutz garantiert wird oder c) dies im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; oder d) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf.
<b>Bern</b> Datenschutzgesetz (KDSG) Datenschutzverordnung (DSV) Direktionsverordnung über Informations-sicherheit und Datenschutz (IDS D) Allgemeine Geschäftsbedingungen des Kantons Bern über die Informations-sicherheit und den Datenschutz (IDS) bei der Erbringung von Informatikdienst-leistungen (AGB IDS)	<a href="https://www.lexfind.ch/fe/tol/22859/versions/191738/de">https://www.lexfind.ch/fe/tol/22859/versions/191738/de</a> <a href="https://www.lexfind.ch/fe/tol/23528/versions/191742/de">https://www.lexfind.ch/fe/tol/23528/versions/191742/de</a> <a href="https://www.lexfind.ch/fe/tol/23879/versions/192396/de">https://www.lexfind.ch/fe/tol/23879/versions/192396/de</a> <a href="https://www.bakm.bag.admin.ch/content/dam/bakm/dokumen-te/de/startseite/themen/rechtsgrundlagen/idsd/1_AGB%20IDS%20IDS%20%20%20%20.pdf">https://www.bakm.bag.admin.ch/content/dam/bakm/dokumen-te/de/startseite/themen/rechtsgrundlagen/idsd/1_AGB%20IDS%20IDS%20%20%20%20.pdf</a>		<b>Art. 16 KDSG Bearbeiten im Auftrag</b> 1 Wer Personendaten im Auftrag einer Behörde bearbeitet, untersteht dem Gesetz wie der Auftraggeber. Zur Bekanntgabe von Personendaten an Dritte bedarf der der ausdrücklichen Zustimmung des Auftraggebers.	<b>Art. 17 KDSG Datensicherung</b> 1 Wer Personendaten bearbeitet, sorgt für ihre Sicherung.  Konkretisierungen in Art. 4 ff. DSV.	<b>Art. 14a KDSG d ins Ausland</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Trotz fehlender Gesetzgebung, die einen angemessenen Schutz gewährleistet, können Personendaten ins Ausland bekannt gegeben werden, wenn: a hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten, b die betroffene Person im Einzelfall eingewilligt hat, c die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt, d die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist, e die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen oder f die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten. 3 Die Aufsichtsstellen muss vor der Bekanntgabe der Personendaten ins Ausland rechtzeitig über die Garantien nach Absatz 2 Buchstabe a informiert werden.
					<b>Art. 14 KDSG c gemeinsame Bestimmung</b> 1 Die Bekanntgabe von Personendaten kann aus überwiegenden öffentlichen oder besonders schützenswerten privaten Interessen verweigert, eingeschränkt oder mit Auflagen verbunden werden. 2 Stehen Personendaten unter dem Schutz besonderer Geheimhaltungsvorschriften, so dürfen sie nur bekanntgegeben werden, wenn der Empfänger einer entsprechenden Geheimhaltungspflicht untersteht.

ERLASSE	AUFRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Freiburg</b> Gesetz über den Datenschutz (DSchG) E-Government-Gesetz  <a href="https://www.legifind.ch/fas/doc/tol/4251/versions/200868/de">https://www.legifind.ch/fas/doc/tol/4251/versions/200868/de</a> <a href="https://www.legifind.ch/fas/doc/tol/33324/versions/200878/de">https://www.legifind.ch/fas/doc/tol/33324/versions/200878/de</a>	<b>Art. 12b DSchG Auslagerung – Grundsätze</b> <p>1 Die Bearbeitung personenbezogener Daten, einschliesslich besonders schützenswerter Daten, kann unter den in diesen Bestimmungen festgelegten Bedingungen ausgelagert werden.</p> <p>2 Die Daten müssen jederzeit auf dem Gebiet der Schweiz oder auf dem Gebiet eines Staates, der einen gleichwertigen Datenschutz gewährleistet, bearbeitet werden.</p> <p>3 Wenn die Auslagerung eine Delegation von Aufgaben an Dritte im Sinne von Artikel 54 der Kantonsverfassung vom 16. Mai 2004 zur Folge hat, gelten besondere Anforderungen gemäss dieser Bestimmung.</p> <p>4 Der Staatstrat unterbreitet der Finanz- und Geschäftsprüfungskommission alle zwei Jahre einen Bericht über die Auslagerung.</p> <b>Art. 12c DSchG Auslagerung – Verantwortung [...]</b> <b>Art. 12d DSchG Auslagerung – Sicherheitsmaßnahmen [...]</b> <b>Art. 12e DSchG Auslagerung – Massnahmen für besonders schützenswerte Personendaten</b> <p>1 Das Bearbeiten von besonders schützenswerten Personendaten bei dem ein konkretes Risiko besteht, dass gegen das Recht der betroffenen Personen verstossen wird, und das Bearbeiten von Daten die einer gesetzlichen oder vertraglichen Geheimhaltungspflicht unterliegen, darf dann ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt ist, so dass dieser auf deren Inhalt keinen Zugriff hat.</p> <p>2 Wenn der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben muss, werden im Auslagerungsvertrag die nötigen besonderen Anforderungen festgelegt, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis des öffentlichen Organs, welches die Daten auslagerst, auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen.</p> <b>Art. 18 DSchG Verantwortung – Auftragsbearbeitung</b> <p>1 Das öffentliche Organ, das Personendaten von einem Auftragsbearbeiter bearbeiten lässt, bleibt für den Datenschutz verantwortlich. Es muss namentlich dem Auftragsbearbeiter die nötigen Weisungen geben und dafür sorgen, dass er die Daten nur für die Ausführung des Auftrags verwendet oder bekanntigt.</p> <p>2 Ist dieses Gesetz auf die beauftragte Drittperson nicht anwendbar und gewährleisten keine anderen gesetzlichen Bestimmungen einen genügenden Datenschutz, so hat das öffentliche Organ den Datenschutz durch einen Vertrag sicherzustellen.</p>	<b>Art. 12c DSchG Auslagerung – Verantwortung</b> <p>1 Das öffentliche Organ, das Daten auslagerst, bleibt für den Schutz der Personendaten, insbesondere für die Vertraulichkeit und die Kontinuität ihrer Aufbewahrung und Nutzung, verantwortlich. Insbesondere: [...]</p> <p>b) gewährleistet es den Schutz und die Sicherheit der Daten und deren eigenen Informationssysteme, indem sie einen Vertrag abschliesst, der mindestens Folgendes beschreibt:</p> <ol style="list-style-type: none"> <li>1. den Gegenstand, die Art, den Zweck und die Dauer der Auslagerung;</li> <li>2. die betroffenen Datenkategorien;</li> <li>3. die Pflichten und Rechte jeder Partei;</li> <li>4. die Rechte und die Kontrollmöglichkeiten der Aufsichtsbehörde im Bereich des Datenschutzes;</li> <li>5. das an den Auftragsbearbeiter gerichtete Verbot, ohne vorherige Genehmigung des für die Datensammlung Verantwortlichen seinesseits einen weiteren Auftragsbearbeiter für die Bearbeitung zu beauftragen;</li> <li>6. die Pflicht des Auftragsbearbeiters, den Verantwortlichen der Datensammlung unverzüglich zu informieren, wenn er aufgrund eines ausländischen Gesetzes oder einer richterlichen Entscheids die Daten einer ausländischen Behörde bekanntgeben muss oder Gefahr läuft, dass er es tun muss.</li> </ol> <p>a) ergreift es die Vorsichtsmaßnahmen, die bei der Wahl des Auftragsbearbeiters, den Weisungen an diesen und der Aufsicht über diesen aufgrund der Umstände geboten sind; [...]</p> <b>Art. 12d DSchG Auslagerung – Sicherheitsmaßnahmen</b> <p>1 Die Universaltheit, die Authentizität, die Verfügbarkeit und die Vertraulichkeit der Personendaten, die von einer Auslagerung betroffen sind, sowie deren ständige Aufbewahrung und Verwendung müssen mit geeigneten organisatorischen und technischen Maßnahmen, die der Entwicklung der verfügbaren Technologien angepasst sind, sichergestellt werden.</p> <p>2 Die Definition von Sicherheitsmaßnahmen berücksichtigt die Gefahren, die das Bearbeiten der fraglichen Daten für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringt.</p> <p>3 Wenn die Auslagerung Daten betrifft, die für den Betrieb der Verwaltung unbedingt nötig sind, muss die Fortführung der ausgelagerten Tätigkeiten bei einem Zwischenfall mit einem angemessenen Dispositiv sichergestellt werden.</p> <b>Art. 22 DSchG Organisatorische und technische Massnahmen</b> <p>1 Das öffentliche Organ, das Personendaten bearbeitet, muss die geeigneten organisatorischen und technischen Massnahmen treffen, um die Daten gegen jedes unerlaubte Bearbeiten zu schützen.</p> <p>2 Der Staatstrat bestimmt die Mindestanforderungen in diesem Bereich. Er holt vorgängig die Stellungnahme der kantonalen Öffentlichkeits- und Datenschutzkommission ein.</p>	<b>Art. 12a DSchG Bekanntgabe ins Ausland</b> <p>1 Personendaten dürfen nur in Staaten bekannt gegeben werden, die einen angemessenen Schutz gewährleisten.</p> <p>2 In Staaten, die keinen angemessenen Schutz gewährleisten, dürfen Personendaten jedoch bekannt gegeben werden, wenn eine der folgenden Bedingungen erfüllt ist:</p> <ol style="list-style-type: none"> <li>a) Hinreichende Garantien, insbesondere vertragliche Garantien, gewährleisten einen angemessenen Schutz im Ausland.</li> <li>b) Die betroffene Person hat im Einzelfall ausdrücklich eingewilligt.</li> <li>c) Die Bearbeitung steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags und es handelt sich um Personendaten des Vertragspartners.</li> <li>d) Die Bekanntgabe ist im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich.</li> <li>e) Die Bekanntgabe ist im Einzelfall erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen.</li> </ol> <p>3 Vor der Bekanntgabe der Daten ins Ausland informiert das öffentliche Organ die kantone Datenschutzbeauftragten über die Garantien nach Absatz 2 Bst. a.</p>	<b>Art. 28 E-GovG Wahren besonderer Geheimnisse</b> <p>1 Das Bearbeiten von Daten, für die eine gesetzliche oder vertragliche Geheimhaltungspflicht gilt, darf nur ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt wird, so dass dieser keinen Zugriff auf ihren Inhalt hat.</p> <p>2 Wenn der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben muss, werden besondere Anforderungen festgelegt, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis der Verwaltungsbehörde, welche die Daten auslager, auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen.</p>	

ERLASSE	AUFRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<p><b>Gef</b> Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)</p> <p>Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD)</p>	<p><a href="https://www.lexfind.ch/fe/de/tot/3180/versions/199485/fr">https://www.lexfind.ch/fe/de/tot/3180/versions/199485/fr</a></p> <p><a href="https://www.lexfind.ch/fe/de/tot/31889/versions/199486/fr">https://www.lexfind.ch/fe/de/tot/31889/versions/199486/fr</a></p> <p><b>Art. 13A) Sous-traitance (art. 37, al. 2, de la loi RIPAD)</b> 1 Le traitement de données personnelles peut être confié à un tiers pour autant qu'une obligation légale ou contractuelle de garder le secret ne l'interdisse. 2 L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même. 3 La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant. 4 Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article. 5 Si l'implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat. 6 Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.</p>	<p><b>Art. 13A(15) Sous-traitance (art. 37, al. 2, de la loi RIPAD) [..]</b> 3 La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant. [..]</p>	<p><b>Art. 37 LIPAD Sécurité des données personnelles</b> 1 Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées. 2 Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter. 3 Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.</p> <p><b>Art. 13 RIPAD Sécurité des données personnelles (art. 37 de la loi)</b> En général 1 Les institutions publiques prennent les mesures organisationnelles et techniques propres à assurer la sécurité des données personnelles. 2 Pour l'administration cantonale, les mesures techniques et organisationnelles nécessaires à la sécurité des données personnelles sont définies notamment par le respect: a) du règlement sur l'organisation et la gouvernance des systèmes d'information et de communication, du 26 juin 2013; b) de l'article 23A, alinéa 5, du règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publicsmédicaux, du 24 février 1999; c) des directives approuvées par la commission de gouvernance des systèmes d'information et de communication; d) des règles et mesures de sécurité édictées par les maîtres de fichiers, les responsables départementaux de la sécurité de l'information et l'office cantonal des systèmes d'information et du numérique<sup>(19)</sup>, sur la base des compétences définies par les règlements visés aux lettres a et b; e) des prescriptions réglementaires et des directives en matière d'archivage. Accès aux systèmes d'information 3 Les institutions publiques tiennent à jour un répertoire des personnes ayant accès aux systèmes d'information contenant des données personnelles</p>	<p><b>Art. 39 LIPAD Communication</b> [..]</p> <p><b>A une corporation ou un établissement de droit public étranger</b> 6 La communication de données personnelles à une corporation ou un établissement de droit public étranger n'est possible que si, cumulativement: a) l'entité requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait à des exigences légales assurant un niveau de protection de ces données équivalent aux garanties offertes par la présente loi; b) la communication des données considérées n'est pas contraire à une loi ou un règlement. 7 En l'absence du niveau de protection des données requis par l'alinéa précédent, la communication n'est possible que si elle n'est pas contraire à une loi ou un règlement et si, alternativement: a) elle intervient avec le consentement explicite, libre et éclairé de la personne concernée ou dans son intérêt manifeste; b) elle est dictée par un intérêt public important manifestement prépondérant reconnu par l'organe requis et que l'entité requérante fournit des garanties fiables suffisantes quant au respect des droits fondamentaux de la personne concernée; c) le droit fédéral ou un traité international le prévoit. [..]</p>	<p><b>VORSCHRIFTEN ZUM GEHEIMNISRECHT</b></p>
<p><b>Glarus</b> Gesetz über den Schutz von Personendaten (DSGG) Datenschutzverordnung (DSVGL)</p>	<p><a href="https://www.lexfind.ch/fe/de/tot/6770/versions/193949/de">https://www.lexfind.ch/fe/de/tot/6770/versions/193949/de</a></p> <p><a href="https://www.lexfind.ch/fe/de/tot/7334/versions/193950/de">https://www.lexfind.ch/fe/de/tot/7334/versions/193950/de</a></p> <p><b>Art. 6 DSGGL Verantwortlichkeit, Auslagerung, Strafbestimmung</b> [..]</p> <p>2 Das Bearbeiten von Personendaten darf an Dritte ausgelagert werden, a. .... b. wenn das den Auftrag vergebende öffentliche Organ dafür sorgt, dass die Daten nur so bearbeitet werden, wie es ihm selbst erlaubt ist, und c. wenn keine Geheimhaltungspflichten entgegenstehen. 3 Die Einhaltung der Bestimmungen über den Beauftragten und die Datensicherheit seitens des Beauftragten Dritten ist mittels Weisungen, Kontrollrechten, Auflagen, Vereinbarungen oder mit andern geeigneten Mitteln sicherzustellen. Der Beauftragte darf die zur Verfügung gestellten Personendaten nur dem Auftraggeber bekannt geben und nicht in eigenem Ermessen bearbeiten, unter Vorbehalt anderslautender Vereinbarung. 4 Wer als Beauftragte Person für das Bearbeiten von Personendaten ohne anderslautende ausdrückliche Ermächtigung des auftraggebenden Organs Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Busse bestraft.</p>	<p><b>Art. 6 DSGGL Verantwortlichkeit, Auslagerung, Strafbestimmung</b> [..]</p> <p>3 Die Einhaltung der Bestimmungen über den Datenschutz und die Datensicherheit seitens des beauftragten Dritten ist mittels Weisungen, Kontrollrechten, Auflagen, Vereinbarungen oder mit andern geeigneten Mitteln sicherzustellen. Der Beauftragte darf die zur Verfügung gestellten Personendaten nur dem Auftraggeber bekannt geben und nicht in eigenem Ermessen bearbeiten, unter Vorbehalt anderslautender Vereinbarung. [..]</p>	<p><b>Art. 8 DSGGL Datensicherheit</b> 1 Wer Personendaten bearbeitet, sorgt durch angemessene organisatorische und technische Vorsehungen für ihre Sicherung vor Verlust sowie vor unbefugter Bearbeitung oder Kenntnisnahme. 2 Der Regierungsrat erlässt hinsichtlich einzuhaltender Mindestanforderungen nach Anhörung insbesondere der mit der Informatik befassten Facheinheit sowie des Landesarchivs ausführende Vorschriften. Konkretisierungen in Art. 1ff. DSVGL.</p>	<p><b>Art. 10a DSGGL Datenübermittlung ins Ausland</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b. die betroffene Person im Einzelfall eingewilligt hat; c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt; d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; g. die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.</p>	<p><b>VORSCHRIFTEN ZUM GEHEIMNISRECHT</b></p>
<p><b>Graubünden</b> Kantonales Datenschutzgesetz (KDSG)</p>	<p><a href="https://www.lexfind.ch/fe/de/tot/9382/versions/49058/de">https://www.lexfind.ch/fe/de/tot/9382/versions/49058/de</a></p> <p><b>Art. 3 KDSG 2. Bekanntgabe in besonderen Fällen</b> 1 Entstehen Anstände zwischen zwei Behörden über die Bekanntgabe von Personendaten, so entscheidet die gemeinsame übergeordnete Instanz. 2 Wer Personendaten im Auftrag einer Behörde bearbeitet, bedarf zur Bekanntgabe von Personendaten an Dritte der ausdrücklichen Zustimmung des Auftraggebers.</p>	<p><b>Art. 2 KDSG Bearbeiten von Personendaten 1. Grundsätze</b> 1 Das Bearbeiten von Personendaten hat die Grundsätze der Rechtmäßigkeit, der Verhältnismäßigkeit, der Zweckmäßigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit zu beachten. 2 Die Vorschriften des Bundesgesetzes für das Bearbeiten von Personendaten durch Bundesorgane finden sinngemäss Anwendung. 3 Soweit das kantonale Datenschutzgesetz und die Ausführungsbestimmungen keine abweichenden oder ergänzenden Bestimmungen enthalten, gelten die Definitionen des Bundesgesetzes sinngemäss.</p>	<p><b>AUSLANDSTRANSFERS</b></p>	<p><b>VORSCHRIFTEN ZUM GEHEIMNISRECHT</b></p>	

ERLASSE	AUFTRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT	
<b>Jura</b> Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE)	<a href="https://www.legifind.ch/fc/fd/to/933/versions/30443/fr">https://www.legifind.ch/fc/fd/to/933/versions/30443/fr</a>	<b>Art. 54 CPDT-JUNE Communication transfrontière</b> 1 Le traitement de données ne peut être confié à un tiers qu'aux conditions suivantes: a) une base légale ou une convention avec le tiers le prévoit; b) le mandant ne peut confier que des traitements qu'il est lui-même en droit d'effectuer; c) aucune obligation légale ou contractuelle dégager le secret ne l'interdit; d) la sécurité des données est assurée. 2 Le mandant demeure responsable de la protection des données; il veille notamment à ce que ne soient pas effectués des traitements autres que ceux qu'il a confiés. 3 Le tiers est assujetti aux mêmes contrôles que le mandant.	<b>Art. 20 CPDT-JUNE Sécurité des données</b> 1 Les entités doivent s'assurer que les données sont protégées contre un emploi abusif en prenant des mesures organisationnelles et techniques appropriées. 2 Les entités veillent à l'intégrité, à la disponibilité et à la confidentialité des données.	<b>Art. 27 CPDT-JUNE Communication transfrontière</b> 1 Des données ne peuvent être communiquées à l'étranger que si les conditions requises par la législation fédérale sur la protection des données sont remplies. 2 Les entités informent le préposé des garanties prises en vertu de cette législation avant la communication de données.		
<b>Luzern</b> Gesetz über den Schutz von Personendaten (DSGLU) Informatikgesetz (IGLU) Verordnung zum Datenschutzgesetz (DSVLU) Verordnung über die Informatik Sicherheit und über die Nutzung von Informatikmitteln (VISLU)	<a href="https://www.legifind.ch/fc/fd/to/1039/versions/18460/de">https://www.legifind.ch/fc/fd/to/1039/versions/18460/de</a> <a href="https://www.legifind.ch/fc/fd/to/10489/versions/55678/de">https://www.legifind.ch/fc/fd/to/10489/versions/55678/de</a> <a href="https://www.legifind.ch/fc/fd/to/1038/versions/18461/de">https://www.legifind.ch/fc/fd/to/1038/versions/18461/de</a> <a href="https://www.legifind.ch/fc/fd/to/1173/versions/62259/de">https://www.legifind.ch/fc/fd/to/1173/versions/62259/de</a>	<b>§ 13 IGLU Auslagerung – Zulässigkeit</b> 1 Die Auslagerung von Informatikdienstleistungen ist zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden. Die finanziellen Vorschriften bleiben vorbehalten. 2 Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt: a. Inhalt der Dienstleistung, b. Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten, c. Verantwortlichkeiten, d. verwendete Techniken, einschliesslich Entwicklung und Wartung, e. Zugriffs- und Zutrittsrechte, f. Sicherheits- und Datenlöschkonzept, g. Standorte der Hardware und der Datenbearbeitung, h. Kontrollrechte, i. Bezug von Dritten, j. Archivierung, k. Rückführung und Löschung der Daten im Fall der Vertragsauflösung. 3 Das auslagernde Organ stellt durch organisatorische oder technische Massnahmen sowie vertraglich sicher, dass die staatliche Aufgabenfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn der Auftragnehmer Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt.	<b>§ 13 IGLU Zulässigkeit</b> 1 [...] 2 Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt: a. Inhalt der Dienstleistung, b. Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten, c. Verantwortlichkeiten, d. verwendete Techniken, einschliesslich Entwicklung und Wartung, e. Zugriffs- und Zutrittsrechte, f. Sicherheits- und Datenlöschkonzept, g. Standorte der Hardware und der Datenbearbeitung, h. Kontrollrechte, i. Bezug von Dritten, j. Archivierung, k. Rückführung und Löschung der Daten im Fall der Vertragsauflösung. 3 [...]	<b>§ 7 DSGLU Datensicherung</b> 1 Organe sorgen durch angemessene technische und organisatorische Massnahmen für die Sicherung von Personendaten. Sie sichern sie insbesondere vor Verlust, Fälschung, Entwendung sowie vor Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte. 2 Der Regierungsrat kann weitere Vorschriften erlassen. Konkretisierung in § 6 DSVLU. Siehe auch § 13 Abs. 3 IGLU; § 12 ff. V VISLU	<b>§ 12a DSGLU Grenzüberschreitende Bekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, nämlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können persönliche Daten nur ins Ausland bekanntgegeben werden, wenn a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten, b. die betroffene Person im Einzelfall eingewilligt hat, c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages steht und es sich um Personendaten des Vertragspartners handelt, d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist, e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen, f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. 3 Der Beauftragte für den Datenschutz muss über die Garantien nach Absatz 2a informiert werden. Der Regierungsrat regelt das Nähere.	
				<b>§ 8a DSVLU Grenzüberschreitende Bekanntgabe</b> 1 Das bekanntgebende Organ informiert den Beauftragten für den Datenschutz vor der grenzüberschreitenden Bekanntgabe über die Garantien nach § 12a Absatz 2a des Datenschutzgesetzes, falls die vorgängige Information nicht möglich, so hat sie unmittelbar nach der Bekanntgabe zu erfolgen. 2 Die Informationspflicht gilt als erfüllt für alle Bekanntgaben, die unter denselben Garantien erfolgen, soweit die Kategorien der Empfänger, der Zweck der Bearbeitung und die Datenkategorien unverändert bleiben. 3 Das bekanntgebende Organ trifft angemessene Massnahmen, um sicherzustellen, dass der Empfänger die Garantien beachtet.		

ERLASSE	AUFTRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Neuenburg</b> Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE)	<a href="https://www.legifind.ch/fc/de/tot/9531/versions/50445/fr">https://www.legifind.ch/fc/de/tot/9531/versions/50445/fr</a>	<b>Art. 54 CPDT-JUNE Communication transfrontière</b> 1 Le traitement de données ne peut être confié à un tiers qu'aux conditions suivantes: a) une base légale ou une convention avec le tiers le prévoit; b) le mandant ne peut confier que des traitements qu'il est lui-même en droit d'effectuer; c) aucune obligation légale ou contractuelle dégager le secret ne l'interdit; d) la sécurité des données est assurée. 2 Le mandant demeure responsable de la protection des données; il veille notamment à ce que ne soient pas effectués des traitements autres que ceux qu'il a confiés. 3 Le tiers est assujetti aux mêmes contrôles que le mandant.	<b>Art. 20 CPDT-JUNE Sécurité des données</b> 1 Les entités doivent s'assurer que les données sont protégées contre un emploi abusif en prenant des mesures organisationnelles et techniques appropriées. 2 Les entités veillent à l'intégrité, à la disponibilité et à la confidentialité des données.	<b>Art. 27 CPDT-JUNE Communication transfrontière</b> 1 Des données ne peuvent être communiquées à l'étranger que si les conditions requises par la législation fédérale sur la protection des données sont remplies. 2 Les entités informer le préposé des garanties prises en vertu de cette législation avant la communication de données.	
<b>Nidwalden</b> Gesetz über den Datenschutz (kDSG)	<a href="https://www.legifind.ch/fc/de/tot/13410/versions/68798/de">https://www.legifind.ch/fc/de/tot/13410/versions/68798/de</a>	<b>Art. 9 kDSG Datenbearbeitung durch Dritte</b> 1 Die Datenbearbeitung kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn: 1. die Daten nur so bearbeitet werden, wie die Auftraggeberin oder der Auftraggeber selbstest tun dürfte; 2. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. 2 Die Auftraggeberin oder der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.	<b>Art. 7 kDSG Datensicherheit</b> 1 Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugte Bearbeitung geschützt werden. 2 Der Regierungsrat erlässt Vorschriften über die Mindestanforderungen an die Datensicherheit.	<b>Art. 6 kDSG Bekanntgabe ins Ausland</b> 1 Daten dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen am gemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können Daten ins Ausland nur bekanntgegeben werden, wenn: 1. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; 2. die betroffene Person im Einzelfall zugestimmt hat; 3. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist. 4. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; 5. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. 3 Die Aufsichtsstelle muss über die Garantien nach Abs. 2 Ziff. 1 informiert werden.	
<b>Obwalden</b> Gesetz über den Datenschutz (DSGOW)	<a href="https://www.legifind.ch/fc/de/tot/13721/versions/69832/de">https://www.legifind.ch/fc/de/tot/13721/versions/69832/de</a>	Keine Angaben im DSGOW. Deshalb gelten sinngemäss die Vorschriften des Bundesgesetzes über den Datenschutz (Art. 2 Abs. 1 DSGOW).	<b>Art. 13 DSGH Bearbeiten im Auftrag</b> 1 Beauftragt das verantwortliche Organ ein anderes öffentliches Organ oder Dritte mit dem Bearbeiten von Personendaten, ist der Datenschutz durch Vereinbarung, Auflagen oder auf andere Weise sicherzustellen. 2 Ohne ausdrückliche anderslautende Ermächtigung darf die beauftragte Stelle Personendaten nur für den Auftraggeber verwenden und nur diesem bekanntgeben.	<b>Art. 14 DSGSH Datensicherung</b> Personendaten sind durch angemessene technische und organisatorische Massnahmen vor Verlust, Entwendung und unbefugtem Bearbeiten zu schützen. <b>§ 3 DSVSH Datensicherung – Allgemeine Massnahmen</b> 1 Das verantwortliche Organ hat eine angemessene Datensicherung zu gewährleisten und Personendaten insbesondere vor folgenden Gefahren zu schützen: a) unbefugte oder zufällige Vernichtung; b) zufälliger Verlust; c) technische Fehler; d) Fälschung, Diebstahl oder widerrechtliche Verwendung; e) unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. 2 Die technischen und organisatorischen Massnahmen müssen verhältnismässig sein und periodisch überprüft werden. 3 Sie tragen insbesondere folgenden Kriterien Rechnung: a) Zweck der Datenbearbeitung; b) Art und Umfang der Datenbearbeitung; c) mögliche Gefährdung der Persönlichkeitrechte betroffener Personen; d) Stand der Technik.	<b>Art. 11b DSGSH Bekanntgabe von Personendaten an Drittstaaten</b> 1 An Drittstaaten dürfen Personendaten unter Vorbehalt von Art. 8 ff. nur bekannt gegeben werden, sofern diese ein angemessenes Datenschutzniveau gemäss Art. 2 Ziff. 2 des Zusatzprotokolls der Europarates vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (SEV Nr. 108) gewährleisten. 2 Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die für die Datenübermittlung von Bedeutung sind. 3 Gewährleistet ein Drittstaat kein angemessenes Datenschutzniveau, so können ihm Personendaten im Einzelfall bekannt gegeben werden, wenn: a) die betroffene Person ohne jeden Zweifel eingewilligt hat; handelt es sich um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, so muss die Einwilligung ausdrücklich sein; b) die Bekanntgabe erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; oder c) die Bekanntgabe zur Wahrung überwiegender öffentlicher Interessen oder zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist. 4 Die Übermittlung unterbleibt, soweit Grund zur Annahme besteht, dass sie gegen die schweizerische Rechtsordnung verstossen würde oder die Übermittlung der ordre public widerspricht. 5 Personendaten können bekannt gegeben werden, wenn im Einzelfall hinreichende vertragliche Garantien einen angemessenen Schutz der betroffenen Person gewährleisten.
<b>Schaffhausen</b> Gesetz über den Schutz von Personendaten (DSGSH) Verordnung über den Schutz von Personendaten (DSVSH)	<a href="https://www.legifind.ch/fc/de/tot/14095/versions/71210/de">https://www.legifind.ch/fc/de/tot/14095/versions/71210/de</a> <a href="https://www.legifind.ch/fc/de/tot/14084/versions/71124/de">https://www.legifind.ch/fc/de/tot/14084/versions/71124/de</a>		<b>§ 4 DSVSH Besondere Massnahmen</b> Das verantwortliche Organ trifft namentlich bei der automatisierten Bearbeitung von Personendaten die geeigneten technischen und organisatorischen Massnahmen, um folgende Ziele zu erreichen: a) Zugangskontrolle: Unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren; b) Benutzerkontrolle: Unbefugten Personen ist die Benutzung von Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren; c) Datenträgerkontrolle: Unbefugten Personen ist das Lesen, Kopieren, Verändern, Zerstören oder Entfernen von Personendatenträgern zu verunmöglichen; d) Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf die Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgaben benötigen; e) Empfängeridentifikation: Empfängerinnen und Empfänger von bekanntzugebenden Personendaten müssen identifiziert werden können.		

ERLASSE	AUFTRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Schwyz</b> Gesetz über die Öffentlichkeit der Verwaltung und den Datenschutz (ÖDSG) Verordnung zum Öffentlichkeits- und Datenschutzgesetz (ÖDSV) Verordnung über die Informations- und Kommunikationstechnologie (IKTV)	<p><b>§ 20 ÖDSG Besondere Formen der Datenbearbeitung – durch Dritte</b></p> <p>1 Lasst ein öffentliches Organ Personendaten durch Dritte bearbeiten, stellt es durch Vereinbarung oder in anderer verbindlicher Weise wirksam sicher, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun durfte. Der Regierungsrat regelt die Einzelheiten.</p> <p>2 Der beauftragte Dritte darf die Personendaten nur im Unterauftragsverhältnis bearbeiten lassen, wenn das öffentliche Organ:</p> <ul style="list-style-type: none"> <li>a) vorgängig seine schriftliche Zustimmung erteilt hat;</li> <li>b) die Einhaltung der Datenschutzpflichten uneingeschränkt einfordern kann;</li> <li>c) seine Kontrollrechte ungehindert ausüben kann.</li> </ul> <p>3 Die Verantwortung für die Datenbearbeitung nach diesem Gesetz bleibt beim öffentlichen Organ. Betroffene Personen haben ihre Rechte gegenüber dem öffentlichen Organ geltend zu machen.</p> <p><b>§ 30 IKTV Auslagerung – Zulässigkeit</b></p> <p>1 Die Auslagerung von ICT-Dienstleistungen ist zulässig, sofern die Vorschriften über den Datenschutz und den Finanzhaushalt sowie die Bestimmungen dieser Verordnung eingehalten werden.</p> <p>2 Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt:</p> <ul style="list-style-type: none"> <li>a) Inhalt der Leistungen der Parteien;</li> <li>b) Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten;</li> <li>c) Verantwortlichkeiten;</li> <li>d) verwendete Techniken, einschliesslich Entwicklung und Wartung;</li> <li>e) Zugriffs- und Zutrittsrechte;</li> <li>f) Sicherheits- und Datenlöschkonzept;</li> <li>g) Standorte der Hardware und der Datenbearbeitung; ...</li> <li>h) Kontrollrechte und Aufsicht;</li> <li>i) Bezug von Dritten;</li> <li>j) Leistungsstörungen und Konventionalstrafe;</li> <li>k) angemessene Massnahmen;</li> <li>l) Aufbewahrung und Archivierung;</li> <li>m) Sicherstellung des Eigentums an Daten und Hilfsprogrammen zur Weiterverwendung bei Auflösung des Vertrages;</li> <li>n) Rückführung und Löschung der Daten im Fall der Vertragsauflösung.</li> </ul> <p>3 Die auslagernde Verwaltungseinheit stellt durch organisatorische, technische und vertragliche Vorkehrungen sicher, dass die kantone Aufgabenerfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn der Auftragnehmer Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt.</p>	<p><b>§ 20 ÖDSG Besondere Formen der Datenbearbeitung – durch Dritte</b></p> <p>1 Lasst ein öffentliches Organ Personendaten durch Dritte bearbeiten, stellt es durch Vereinbarung oder in anderer verbindlicher Weise wirksam sicher, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte. Der Regierungsrat regelt die Einzelheiten.</p> <p>2 Der beauftragte Dritte darf die Personendaten nur im Unterauftragsverhältnis bearbeiten lassen, wenn das öffentliche Organ:</p> <ul style="list-style-type: none"> <li>a) vorgängig seine schriftliche Zustimmung erteilt hat;</li> <li>b) die Einhaltung der Datenschutzpflichten uneingeschränkt einfordern kann;</li> <li>c) seine Kontrollrechte ungehindert ausüben kann.</li> </ul> <p>3 Die Verantwortung für die Datenbearbeitung nach diesem Gesetz bleibt beim öffentlichen Organ. Betroffene Personen haben ihre Rechte gegenüber dem öffentlichen Organ geltend zu machen.</p>	<p><b>§ 18 ÖDSG Bekanntgabe ins Ausland</b></p> <p>Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.</p>	<p>Siehe § 30 Abs. 2 lit. b) IKTV</p> <p><b>§ 3 ÖDSG – Spezialgesetzgebung</b></p> <p>1 Spezielle Bestimmungen anderer Erlasse, nach denen bestimmte Informationen als geheim gelten oder welche den Zugang zu amtlichen Dokumenten oder das Bearbeiten von Personendaten abweichend regeln, gehen diesem Gesetz vor.</p> <p>2 Das anwendbare Verfahrensrecht regelt die Bearbeitung von Personendaten in der Zivil-, Straf- und Verwaltungsrechtspflege. Es bleibt auch nach dem Abschluss des Verfahrens vorbehalten.</p>	

ERLASSE	AUFTRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Solothurn</b> Informations- und Datenschutzgesetz (InfoDG) Informations- und Datenschutzverordnung (InfoDV) Allgemeine Geschäftsbedingungen des Kantons Solothurn über die Informationssicherheit und den Datenschutz bei der Erbringung von Informatikdienstleistungen (AGB ISDS)	<a href="https://www.lexfind.ch/fe/de/tol/1589/versions/79357/de">https://www.lexfind.ch/fe/de/tol/1589/versions/79357/de</a> <a href="https://www.lexfind.ch/fe/de/tol/15873/versions/78968/de">https://www.lexfind.ch/fe/de/tol/15873/versions/78968/de</a> <a href="https://rb.su.ch/rbde/lehrgang/18x_rispub-publication/publication/03pub-publication%5D=44242&amp;2cHash=2461fd8da52423f9fb9eecc2e04a5">https://rb.su.ch/rbde/lehrgang/18x_rispub-publication/publication/03pub-publication%5D=44242&amp;2cHash=2461fd8da52423f9fb9eecc2e04a5</a>	<b>§ 17 InfoDG Datenbearbeiten durch Dritte</b> 1 Lässt eine Behörde Personendaten durch Dritte bearbeiten, stellt sie den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicher.	<b>§ 16 InfoDG Grundsätze</b> 1 Wer Personendaten bearbeitet, a) [...] b) [...] c) schützt die Daten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten. 2 [...] 3 [...]	<b>§ 21bis InfoDG Grenzüberschreitende Bekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet wird, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a) hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b) die betroffene Person im Einzelfall eingewilligt hat; c) die Bekanntgabe im Einzelfall entweder für die Wahrung eines wichtigen öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; d) die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; e) die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	
<b>St. Gallen</b> Datenschutzgesetz (DSG) Verordnung über die Informatik Sicherheit (VI)	<a href="https://www.lexfind.ch/fe/de/tol/16872/versions/83364/de">https://www.lexfind.ch/fe/de/tol/16872/versions/83364/de</a> <a href="https://www.lexfind.ch/fe/de/tol/15457/versions/185092/de">https://www.lexfind.ch/fe/de/tol/15457/versions/185092/de</a>	<b>Art. 9 DSG Bearbeitung durch Dritte</b> 1 Das öffentliche Organ kann die Bearbeitung von Personendaten an Dritte übertragen, wenn die Übertragung nicht durch Gesetz oder Verordnung ausgeschlossen ist und die beauftragten Dritten Gewähr für die datenschutzwidrige einwandfreie Bearbeitung bieten. 2 Es stellt die Einhaltung des Datenschutzes sicher und legt insbesondere fest, dass die Personendaten: a) nur so bearbeitet werden, wie das öffentliche Organ es selbst tun darf; b) nach den für das öffentliche Organ geltenden gesetzlichen Bestimmungen bearbeitet werden; c) vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten gesichert werden. 3 Es prüft durch geeignete regelmäßige Kontrollen, ob der Datenschutz eingehalten wird. Stellt es die Nichteinhaltung von Auflagen nach Abs. 2 dieser Bestimmung oder Verstöße gegen andere Datenschutzzuschreibungen fest, macht es die Übertragung rückgängig. 4 Die Weiterübertragung der Datenbearbeitung bedarf der vorgängigen schriftlichen Zustimmung des auftraggebenden öffentlichen Organs.	<b>Art. 9 DSG Bearbeitung durch Dritte</b> 1 [...] 2 [...] 3 [das öffentliche Organ] prüft durch geeignete regelmäßige Kontrollen, ob der Datenschutz eingehalten wird. Stellt es die Nichteinhaltung von Auflagen nach Abs. 2 dieser Bestimmung oder Verstöße gegen andere Datenschutzzuschreibungen fest, macht es die Übertragung rückgängig. 4 [...]	<b>Art. 4 DSG Grundsätze</b> 1 [...] 2 [...] 3 [das öffentliche Organ] trifft organisatorische und technische Massnahmen zur Sicherung der Daten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten.  Konkretisierungen in VI:	<b>Art. 16 DSG Bekanntgabe ins Ausland</b> 1 Die Bekanntgabe von Personendaten ins Ausland richtet sich sachgemäß nach den Bestimmungen der Bundesgesetzgebung über den Datenschutz. 2 Das öffentliche Organ informiert vor der Bekanntgabe die zuständige Fachstelle für Datenschutz über die von der Bundesgesetzgebung geforderten Garantien, wenn der Staat nicht auf der von der oder vom eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten veröffentlichten Liste der Staaten mit angemessener Datenschutzgesetzgebung aufgeführt ist. 3 Die kantonale Fachstelle für Datenschutz beschafft bei der oder beim eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten Informationen über den Datenschutz im Ausland. Sie stellt die Informationen zur Verfügung: a) den öffentlichen Organen in ihrem Zuständigkeitsbereich; b) den Fachstellen der Gemeinden zur Weiterleitung an die öffentlichen Organe in deren Zuständigkeitsbereich.

ERLASSE	AUFTAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
Tessin  Legge sulla protezione dei dati personali (LPDP)  Regolamento di applicazione alla legge cantonale sulla protezione dei dati personali (RLPD)	<a href="https://www.lexfind.ch/fe/ide/tol/21501/versions/118492/de">https://www.lexfind.ch/fe/ide/tol/21501/versions/118492/de</a> <a href="https://www.lexfind.ch/fe/ide/tol/21427/versions/11791/de">https://www.lexfind.ch/fe/ide/tol/21427/versions/11791/de</a>	<b>Art. 16 LPDP Elaborazione su mandato</b> 1 Se l'organo responsabile incarica un altro organo pubblico o terzi di elaborare dati personali, la protezione dei dati secondo la presente legge deve essere garantita da condizioni, convenzioni o in altro modo. 2 Senza esplicita autorizzazione derogante, il servizio mandatario può utilizzare dati personali soltanto per il mandante e trasmetterli solo a quest'ultimo.	<b>Art. 17 LPDP Sicurezza</b> Chi elabora dati personali deve prendere misure appropriate di sicurezza contro la perdita, il furto, l'elaborazione e la consultazione illecita.	<b>Art. 14a LPDP Trasmissione all'estero</b> 1 I dati personali non possono essere trasmessi all'estero qualora la personalità della persona interessata possa subire grave pregiudizio, dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata. 2 Se manca una legislazione che assicura una protezione adeguata, dati personali possono essere trasmessi all'estero soltanto se: a) garanzie sufficienti, segnatamente contrattuali, assicurano una protezione adeguata all'estero; b) la persona interessata ha dato il suo consenso nel caso specifico; c) nel caso specifico la trasmissione è indispensabile per tutelare un interesse pubblico preponderante oppure per accertare, esercitare o far valere un diritto in giustizia; d) nel caso specifico la trasmissione è necessaria per proteggere la vita o l'incolumità fisica della persona interessata; e) la persona interessata ha reso i dati accessibili a chiunque e non si è opposta formalmente alla loro elaborazione. 3 L'organo responsabile informa l'incaricato cantonale della protezione dei dati sulle garanzie ai sensi del capoverso 2 lettera a). Il Consiglio di Stato disciplina i particolari. 4 Laddove una protezione adeguata sia assicurata, la trasmissione è lecita se sono adempiute le condizioni valide per la trasmissione di dati in Svizzera.	
Thurgau  Gesetz über den Datenschutz (DSG)  Verordnung des Regierungsrates über den Datenschutz (DSV)  Informatikreglement (ITR)	<a href="https://www.lexfind.ch/fe/ide/tol/17664/versions/192915/de">https://www.lexfind.ch/fe/ide/tol/17664/versions/192915/de</a> <a href="https://www.lexfind.ch/fe/ide/tol/17970/versions/184579/de">https://www.lexfind.ch/fe/ide/tol/17970/versions/184579/de</a> <a href="https://www.lexfind.ch/fe/ide/tol/18444/versions/201883/de">https://www.lexfind.ch/fe/ide/tol/18444/versions/201883/de</a>	<b>§ 12 DSG Bearbeitung durch Dritte</b> 1 Werden Personendaten durch Dritte bearbeitet, ist der Datenschutz im Sinne dieses Gesetzes vom verantwortlichen Organ durch Vertrag oder Verfügung sicherzustellen. 2 Ohne ausdrückliche Ermächtigung darf der Dritte Personendaten nur für das verantwortliche Organ verwenden und nur diesem bekanntgeben.	<b>§ 13 DSG Datensicherung</b> 1 Wer Personendaten bearbeitet, sorgt für deren angemessene Sicherung vor Verlust, Entwendung, unbefugter Bearbeitung oder Kenntnisnahme.	<b>§ 12a LPDP Obligo di informare</b> 1 L'organo responsabile che intende trasmettere dati personali all'estero deve rispettare i principi generali della LPDP e accertarsi preventivamente dell'adeguatezza della protezione dei dati nello Stato di destinazione. 2 Prima della trasmissione all'estero, esso informa l'incaricato sulle garanzie e sulle regole di protezione dei dati ai sensi dell'art. 14 cpv. 2 lett. a LPDP. 3 L'obbligo di informare è considerato soddisfatto se i dati sono trasmessi mediante contratto modello o clausole standard allestiti o riconosciuti dall'incaricato e se l'organo responsabile informa in modo generale l'incaricato dell'impiego di tali contratti modello o clausole standard. 4 L'incaricato pubblica un elenco di tali contratti modello o clausole standard. 5 L'organo responsabile può applicare anche altre garanzie, quali una concezione specifica di protezione dei dati o clausole c) contenute in altri contratti; queste garanzie speciali devono assicurare un livello di protezione adeguato. 6 L'organo responsabile prende misure adeguate per garantire che il destinatario rispetti le garanzie e le regole sulla protezione dei dati. 7 L'incaricato esamina le garanzie e le regole sulla protezione dei dati che gli sono state comunicate (art. 14 cpv. 2 LPDP) e comunica il risultato del suo esame all'organo responsabile entro 30 giorni dalla ricezione dell'informazione.	
Uri  Gesetz über den Schutz von Personendaten (DSG)	<a href="https://www.lexfind.ch/fe/ide/tol/17774/versions/87634/de">https://www.lexfind.ch/fe/ide/tol/17774/versions/87634/de</a>		<b>§ 13 DSG Massnahmen</b> 1 Das verantwortliche Organ hat eine angemessene Datensicherheit zu gewährleisten und trifft Massnahmen zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Datenexistenz und Nachvollziehbarkeit. 2 Personendaten sind vor folgenden Gefahren zu schützen: 1. unbefugte Vernichtung; 2. zufälliger Verlust; 3. technische Fehler; 4. Fälschung, Diebstahl oder widerrechtliche Verwendung; 5. unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. 3 Die technischen und organisatorischen Massnahmen müssen angemessen sein. Insbesondere haben sie folgenden Kriterien Rechnung zu tragen: 1. Zweck der Datenbearbeitung; 2. Art und Umfang der Datenbearbeitung; 3. Einschätzung der möglichen Risiken für die betroffenen Personen; 4. aktueller Stand der Technik. 4 Die Massnahmen sind von der Aufsichtsstelle periodisch zu überprüfen	<b>§ 9a DSG Grenzüberschreitender Datenverkehr</b> 1 Personendaten dürfen an Empfänger, welche der Rechtsnordheit von Staaten oder Organisationen unterliegen, die nicht Vertragspartei des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sind, nur übermittelt werden, wenn diese Staaten oder Organisationen einen angemessenen Schutz für die beabsichtigte Datenübermittlung bieten. 2 Vorbehalten bleiben die Zustimmung der betroffenen Person im Einzelfall und Artikel 2 Absatz 2 des Zusatzprotokolls vom 8. November 2001 zum Abkommen gemäss Absatz 1.	
			<b>Artikel 11 DSG Datensicherung</b> Wer Personendaten bearbeitet, sorgt für ihre Sicherung vor Verlust, Entwendung, unbefugter Bearbeitung oder Kenntnisnahme.	<b>§ 3 DSV Angemessener Datenschutz</b> 1 Ein angemessener Datenschutz im grenzüberschreitenden Datenverkehr ist dann gegeben, wenn im Empfängerstaat ein adäquates Datenschutzniveau sichergestellt ist. 2 Ein solches liegt unter Berücksichtigung aller Umstände insbesondere dann vor, wenn: 1. die Grund- und Menschenrechte eingehalten werden, 2. das Datenschutzniveau europäischem Standard entspricht.	
				<b>Artikel 8a DSG Bekanntgabe von Personendaten ins Ausland</b> 1 Personendaten dürfen ausländischen Stellen der Europäischen Union sowie Vertragsstaaten des Abkommens über den europäischen Wirtschaftsraum bekannt gegeben werden, wenn die Voraussetzungen erfüllt sind, die die Bekanntgabe von Daten im Inland erfüllt sein müssen. 2 Drittstaaten dürfen Personendaten nur bekannt geben werden, wenn zusätzlich zu den Voraussetzungen nach Absatz 1 feststeht, dass darüber die Persönlichkeit der betroffenen Person nicht schwerwiegend gefährdet wird. Namentlich muss die Gesetzgebung des ersuchenden Drittstaats einen Datenschutz gewährleisten, der dem vorliegenden Gesetz entspricht. Der ersuchende Drittstaat hat das nachzuweisen. 3 Im Zweifelsfall entscheidet die beauftragte Person für Datenschutz, ob die datenschutzrechtlichen Voraussetzungen für den Datenaustausch erfüllt sind.	

ERLASSE	AUFRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Waadt</b> Loi sur la protection des données personnelles (LPrD) Règlement d'application de la loi du 11 septembre 2007 sur la protection des données personnelles (RLPrD)	<b>Art. 18 LPrD Traitement des données par un tiers</b> 1 Le traitement de données peut être confié à un tiers aux conditions cumulatives suivantes: a. le traitement par un tiers est prévu par la loi ou par un contrat; b. le responsable du traitement est légitimé à traiter lui-même les données concernées; c. aucune obligation légale ou contractuelle de garder le secret ne l'interdit. 2 Le tiers est responsable de la sécurité des données qu'il traite.		<b>Art. 10 LPrD Sécurité</b> 1 Le responsable du traitement prend les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, soit notamment contre leur perte, leur destruction, ainsi que tout traitement illicite.	<b>Art. 17 LPrD Communication transfrontière de données</b> 1 La communication vers un pays tiers de données personnelles faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat. 2 L'alinéa précédent n'est pas applicable: a. si la personne concernée a donné son consentement, qui doit dans tous les cas être explicite; b. si la communication de données est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures pré-contractuelles prises à la demande de la personne concernée; c. si la communication est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers; d. si la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public, soit à la constatation, l'exercice ou la défense d'un droit en justice; e. si la communication est, en l'espèce nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée; f. si la communication intervient d'un registre public qui, en vertu de dispositions légales ou réglementaires, est destiné à l'information du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier; g. si des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger.	
<b>Wallis</b> Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (GIDA) Ausführungsreglement zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (ARGIDA)	<b>Art. 29 GIDA Bearbeiten im Auftrag</b> 1 Beauftragt der Inhaber der Datensammlung einen Dritten mit dem Bearbeiten von Daten, muss er dafür sorgen, dass der Schutz dieser Informationen und des Bearbeitungsergebnisses gemäss den obengenannten Bestimmungen gewährleistet ist.		<b>Art. 21 GIDA Datensicherheit</b> 1 Die Behörde, die Personendaten bearbeitet oder ein Datennetzwerksnetz zur Verfügung stellt, sorgt für die Echtheit, die Zuverlässigkeit, die Integrität und die Benutzbarkeit der Daten, um einen angemessenen Datenschutz zu gewährleisten. Insbesondere schützt sie die Systeme vor folgenden Risiken: a) zufällige oder unbefugte Vernichtung; b) zufälliger Verlust; c) technische Fehler; d) Fälschung, Diebstahl oder widerrechtliche Verwendung; e) unbefugtes Andern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. 2 Die technischen und organisatorischen Massnahmen müssen angemessen sein. Insbesondere tragen sie folgenden Kriterien Rechnung: a) Zweck der Datenbearbeitung; b) Art und Umfang der Datenbearbeitung; c) Einschätzung der möglichen Risiken für die betroffenen Personen; d) gegenwärtiger Stand der Technik. 3 Diese Massnahmen sind periodisch zu überprüfen.	<b>Art. 25 GIDA Grenzüberschreitende Bekanntgabe von Daten</b> 1 Es dürfen keinerlei Daten bekannt gegeben werden, wenn der Empfänger der Rechtshoheit von Staaten oder Organisationen unterliegt, die kein angemessenes Schutzniveau für die beabsichtigten Datenumübermittlung gewährleisten. 2 Bei fehlendem angemessenem Schutz können personenbezogene Daten ausschliesslich unter einer der folgenden Bedingungen ins Ausland mitgeteilt werden: a) Die betroffene Person hat für die vorgesehene Datenübermittlung ihre vorgängige und ausdrückliche Einwilligung gegeben; b) die Bekanntgabe ist zur Wahrung eines überwiegenden öffentlichen Interesses unerlässlich; c) die Bekanntgabe ist für die Feststellung, die Ausübung oder die Verteidigung eines Rechtes vor Gericht unerlässlich; d) die Bekanntgabe ist notwendig, um das Leben oder die körperliche Integrität der betroffenen Person oder einer Drittperson zu schützen; e) die Bekanntgabe ist für den Abschluss oder die Erfüllung eines Vertrages unerlässlich und die bearbeiteten Daten betreffen den Vertragspartner; f) hinreichende, insbesondere vertragliche Garantien gewährleisten ein angemessenes Schutzniveau fürs Ausland. 3 Der Beauftragte muss die in Absatz 2 Buchstabe f vorgesehenen Garantien genehmigen.	<b>Art. 27 GIDA Weitere Einschränkungen der Bekanntgabe der Daten</b> 1 [...] 2 Stehen Personendaten unter dem Schutz des Berufs- oder Amtsgeheimnisses, können sie nur bekannt gegeben werden, wenn der Empfänger einer gleichwertigen Geheimhaltungspflicht untersteht. 3 Gesetzliche Bestimmungen, welche die Zustimmung der betroffenen Person verlangen, bleiben vorbehalten.

ERLASSE	AUFTRAGSBEARBEITUNG	KONTROLLRECHTE	ANFORDERUNGEN AN DATENSICHERHEIT	AUSLANDSTRANSFERS	VORSCHRIFTEN ZUM GEHEIMNISRECHT
<b>Zug</b> Datenschutzgesetz (DSG) Verordnung über die Informationssicherheit von Personendaten (VIP)	<a href="https://www.leafind.ch/fe/fe/tol/20055/versions/190121/de/">https://www.leafind.ch/fe/fe/tol/20055/versions/190121/de/</a> <a href="https://www.leafind.ch/fe/fe/tol/21100/versions/192334/de/">https://www.leafind.ch/fe/fe/tol/21100/versions/192334/de/</a>	<b>§ 6 DSG Auftragsdatenbearbeitung</b> 1 Ein Organ kann das Bearbeiten von Personendaten Dritten übertragen, wenn a) die Personendaten nur so bearbeitet werden, wie es das Organ selbst tun darf; und b) keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. 2 Das Organ stellt mittels Auflagen, Vereinbarungen oder in anderer Weise sicher, dass die Auftragsdatenbearbeiterin oder der -bearbeiter die Informationssicherheit gewährleistet und die Rechte der betroffenen Person wahrt. 3 Das Organ bleibt für den gesetzmässigen Umgang mit den Personendaten verantwortlich. 4 Die Auftragsdatenbearbeiterin oder der -bearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Organs einer anderen Auftragsdatenbearbeiterin oder einem anderen -bearbeiter übertragen.	<b>§ 7 DSG Informationssicherheit</b> 1 Die Organe sorgen durch angemessene technische und organisatorische Massnahmen für die Sicherheit aller Personendaten. Personendaten sind insbesondere vor Verlust, Fälschung, Entwendung, Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern. 2 Der Regierungsrat erlässt innerhalb eines Jahres nach Inkrafttreten dieses Gesetzes entsprechende Vorschriften, insbesondere über die Sicherheitsgrundsätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches.	<b>§ 10a DSG Grenzüberschreitende Datenbekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person gefährdet wird. Eine Gefährdung liegt insbesondere bei Fehlen einer Gesetzgebung vor, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung gemäss Abs. 1, dürfen Personendaten ins Ausland nur bekanntgegeben werden, wenn eine der folgenden Voraussetzungen erfüllt ist: a) hinreichende Garantien, insbesondere durch Vertrag, gewährleisten einen angemessenen Schutz im Ausland; über diese Garantien muss die Datenschutzstelle vor der Bekanntgabe der Daten ins Ausland informiert werden; b) die betroffene Person hat im Einzelfall ausdrücklich eingewilligt; c) die Bekanntgabe ist im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich; d) die Bekanntgabe im Einzelfall ist erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen. 3 Eine Datenbekanntgabe ins Ausland darf nicht erfolgen, wenn dadurch in schwerwiegender Weise gegen die öffentliche Ordnung verstossen würde.	
<b>Zürich</b> Gesetz über die Information und den Datenschutz (IDG) Gesetz über die Auslagerung von Informatikdienstleistungen (GAVI) Verordnung über die Information und den Datenschutz (IDV) Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen Allgemeine datenschutzwichtige Geschäftsbedingungen bei der Datenbearbeitung durch Dritte	<a href="https://www.leafind.ch/fe/fe/tol/21437/versions/188522/de/">https://www.leafind.ch/fe/fe/tol/21437/versions/188522/de/</a> <a href="https://www.leafind.ch/fe/fe/tol/21874/versions/20873/de/">https://www.leafind.ch/fe/fe/tol/21874/versions/20873/de/</a> <a href="https://www.leafind.ch/fe/fe/tol/21875/versions/20875/de/">https://www.leafind.ch/fe/fe/tol/21875/versions/20875/de/</a> <a href="https://www.zh.ch/bilder-dokumente/organisation/finanzdirektion/agb_datenbearbeitung_agb_auslagerung_idv.pdf">https://www.zh.ch/bilder-dokumente/organisation/finanzdirektion/agb_datenbearbeitung_agb_auslagerung_idv.pdf</a> <b>§ 6. IDG Bearbeiten im Auftrag</b> 1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht. 2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.	<b>§ 6. IDG Bearbeiten im Auftrag</b> 1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht. 2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.	<b>§ 7. IDG Informationssicherheit</b> 1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen. 2 Die Massnahmen richten sich nach den folgenden Schutzzwecken: a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen, b. Informationen müssen richtig und vollständig sein, c. Informationen müssen bei Bedarf vorhanden sein, d. Informationsbearbeitungen müssen einer Person zugerechnet werden können, e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein. 3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.	<b>§ 19. IDG Bekanntgabe von Informationen – Grenzüberschreitend</b> 1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen. 2 Die Massnahmen richten sich nach den folgenden Schutzzwecken: a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen, b. Informationen müssen richtig und vollständig sein, c. Informationen müssen bei Bedarf vorhanden sein, d. Informationsbearbeitungen müssen einer Person zugerechnet werden können, e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein. 3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.	<b>§ 3. GAVI Amtsgesheimnis und Datenschutz</b> 1 Das öffentliche Organ darf besondere Personendaten im Sinne des Gesetzes über die Information und den Datenschutz und solche, die im Interesse des Staates der Geheimhaltung unterliegen, privatrechtlich organisierten Unternehmen nur dann zur Bearbeitung zugänglich machen, wenn sie durch organisatorische und technische Massnahmen vor unbefugter Einsichtnahme geschützt sind. Es stellt sicher, dass solche Daten ausschliesslich von Mitarbeitenden des Unternehmens bearbeitet werden, die diesbezüglich seinem Kontroll- und Weisungsrecht unterstellt und als Hilfspersonen an das Amtsgesheimnis sowie allfällige Berufs- oder Spezialgeheimnisse gebunden sind. 2 Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz über das Bearbeiten von Daten im Auftrag.



Danke  
Merci  
Grazie  
Engraziel