HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Niclas Wagner

Ein Vergleich von nationalen und internationalen Verwendungsmöglichkeiten des Werkzeugs eDiscovery in der M365 Cloud und mögliche technische Einschränkungen zur Gewährleistung des Datenschutzes

Mittweida, 2022

Fakultät Angewandte Computer- und
Biowissenschaften

BACHELORARBEIT

Ein Vergleich von nationalen und internationalen Verwendungsmöglichkeiten des Werkzeugs eDiscovery in der M365 Cloud und mögliche technische Einschränkungen zur Gewährleistung des Datenschutzes

Autor:
Herr
Niclas Wagner

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w4-B

Erstprüfer:
Prof. Ronny Bodach

Zweitprüfer:
M.Sc. Stefan Schildbach

Einreichung:
Mittweida, 12. September 2022

Verteidigung/Bewertung:
Mittweida, 2022

Faculty Applied Computer Sciences & Biosciences

BACHELOR THESIS

A comparison between national and international use cases of the tool eDiscovery in the M365 cloud and possible technical limitations to ensure data privacy

author:
Mr.
Niclas Wagner

course of studies:
General and Digital Forensic Science

seminar group:
FO19w4-B

first examiner:
Prof. Ronny Bodach

second examiner:
M.Sc. Stefan Schildbach

submission:
Mittweida, 12. September 2022

defence/ evaluation:
Mittweida, 2022

Bibliografische Beschreibung:

Wagner, Niclas:
Ein Vergleich von nationalen und internationalen Verwendungsmöglichkeiten des Werkzeugs eDiscovery in der M365 Cloud und mögliche technische Einschränkungen zur Gewährleistung des Datenschutzes. - 2022. - VI, 50, S.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022

Referat:

Die vorliegende Arbeit befasst sich mit einem Vergleich zwischen nationalen und internationalen Verwendungsmöglichkeiten des Werkzeugs eDiscovery in der M365 Cloud. Dabei werden verschiedene technische Einschränkungen vorgestellt, welche die Datenschutzrechtlich konforme Nutzung dieses Werkzeuges ermöglich sollen.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

NIST	National Institute of Standards and Technology
ENISA	European Network and Information Security Agency
CSA	Cloud Security Alliance
EDRM	Electronic Discovery Reference Model
ESI	Electronically stored information
DSGVO	Datenschutzgrundverordnung
BDSG	Bundesdatenschutzgesetz
FISA	Foreign Intelligence Surveillance Act

1 Übersicht

1.1 Motivation

Besonders in den letzten Jahren ist die Nutzung von Cloud-Diensten fast schon zur Selbstverständlichkeit geworden. Besonders in großen, multinationalen Organisationen sind diese kaum mehr wegzudenken und sorgen für einen effektiveren und einfacheren Arbeitsalltag.[1]

Mit der Implementierung von Cloud-Diensten entstehen aber auch neue Herausforderungen in den Organisationen. So ist beispielsweise das Aufspüren von relevanten Dokumenten in der Cloud für Gerichtsprozesse von großer Bedeutung. Dies ist allerdings aufgrund der mitunter großen Datenmengen innerhalb der Cloud nicht trivial. [2]

Von verschiedenen Cloud Anbietern gibt es bereits Möglichkeiten, diese Herausforderungen anzugehen. In der Microsoft Cloud gibt es etwa das Werkzeug eDiscovery, welches für diese und darüber hinaus noch andere Verwendungsszenarien eingesetzt werden kann [3]. Durch eine verstärkt aufkommende Datenschutzbewegung, besonders in den letzten Jahren, stellt sich hier auch die Frage, inwieweit diese Verwendungsmöglichkeiten datenschutzkonform sind. Datenschutz als solches muss eine große Bedeutung haben, sei es nun im kleineren privaten Umfeld oder in einer größeren kommerziellen Umgebung.

1.2 Zielsetzung

In der vorliegenden Arbeit wird sich in Bezug auf die Fragestellung damit auseinandergesetzt, inwiefern sich verschiedene Verwendungsmöglichkeiten des Werkzeugs eDiscovery in Ländern unterscheiden und welche Datenschutzrechtlichen Besonderheiten betrachtet werden müssen.

Hierfür werden verschiedene Begrifflichkeiten hinsichtlich der Cloud-Dienste und eDiscovery definiert und erklärt, so auch technische Einschränkungen des letzteren. Ebenso wird auf den Datenschutz und seine Grundsätze eingegangen.

Das Hauptziel ist dennoch die Gegenüberstellung verschiedener Verwendungs-möglichkeiten des Werkezuges eDiscovery in der Microsoft Cloud. Hier sollen auch technische Möglichkeiten erkundet werden, um das Gewährleisten des Datenschutzes sicherzustellen. Der Datenschutz soll hierbei nicht als pure Idee betrachtet werden, vielmehr geht es um die tatsächlichen Datenschutzregelungen der einzelnen Länder.

2 Grundlagen und Begriffsdefinition

In diesem Kapitel werden im Folgenden Begrifflichkeiten definiert und erläutert, welche in der Fragestellung erwähnt werden und diese genau beschreiben. Die folgenden Erklärungen sollen somit als Grundlagenwissen für die Beantwortung der Fragestellung der Bachelorarbeit dienen.

2.1 Der Begriff Cloud

Die Notwendigkeit den Begriff der Cloud zu betrachten, ergibt sich aus dem simplen Grund, dass die Anwendung des in dieser Arbeit thematisierten Werkzeugs in einer Cloud erfolgt. Das Wissen über die Funktionsweise und das Erläutern verschiedener Verwendungsmöglichkeiten ist für das Verständnis der Nutzung des Werkzeugs eDiscovery und somit für das Verständnis der Arbeit wichtig.

2.1.1 Definition Cloud

Eine einheitliche, allgemeingültige Definition des Begriffes Cloud Computing, im Allgemeinen auch zu „Cloud“ abgekürzt, existiert bislang noch nicht. Die verwendeten Definitionen, welche bisher im wissenschaftlichen Arbeiten verwendet werden, ähneln sich zwar, sind allerdings aufgrund ihrer Variationen nicht eineindeutig.[4]

Runtergebrochen ist die Cloud ein Begriff, hinter der sich ein globales Netzwerk von Servern verbirgt, welche alle eine eigene Funktion besitzen. Sie, die Cloud, ist dabei keine physische Größe, sondern ein großes, global angelegtes Netzwerk von Servern, welche miteinander verbunden sind und wie ein Ökosystem funktionieren. [5]

Eine genaue Definition von Cloud Computing, welche auch am häufigsten in Fachkreisen verwendet wird, ist die des National Institute of Standards and Technology (NIST), der Standardisierungsstelle der Vereinigten Staaten von Amerika. Ebenjene Definition wird auch in Europäischen Behörden wie der European Network and Information Security Agency (ENISA) übernommen. [4]

Cloud Computing oder die Cloud, ist nach der Definition des NIST ein Modell. Bei Bedarf bietet dieses Modell einen einfachen, jederzeit verfügbaren Zugriff über das Internet auf einen geteilten Pool, in welchem verschiedene konfigurierbar Rechenressourcen zur

Nutzung bereitstehen. Diese Ressourcen umfassen etwa Server, Speichersysteme oder Anwendungen. [6]

Das besondere hierbei ist, dass der Zugriff und die Nutzung dieser Rechenressourcen mit geringer Interaktion zu dem Anbieter der Dienste realisiert werden kann und dass die Rechenressourcen darüber hinaus schnell und mit wenig Managementaufwand bereitgestellt werden können. Solange eine Netzwerkverbindung eines Gerätes besteht, kann über diese auf die Dienste der Cloud zugegriffen werden. [6]

Ein Cloud Service wird dabei, laut NIST durch verschiedene, im folgenden aufgezählten Attribute charakterisiert. [6]

On-demand Self Service: Die Bereitstellung der Ressourcen, welche in dem Pool enthalten sind, auf welchen der Cloud Service zugreift, geschieht automatisch. Eine Kommunikation oder ähnliches mit dem Service Provider, hier Cloud Anbieter, gibt es nicht. [6]

Broad Network Access: Die nutzbaren Ressourcen der Cloud sind über das Netz durch Standardmechanismen, wie etwa das Einloggen im Netz verfügbar und nicht an bestimmte Clients gebunden. [6]

Ressource Pooling: Die Ressourcen, welche der Service Provider zur Verfügung stellt, liegen in einem Pool vor. Aus diesem Pool können sich verschiedene Anwender bedienen und die Ressourcen nutzen. Dies wird auch Multi Tenant Modell genannt. Die Anwender haben dabei keine Informationen wo sich die einzelnen Ressourcen geografisch befinden und gespeichert werden. Es gibt jedoch über vertragliche Regelungen die Option, dass der Speicherort beispielsweise die Region oder das Land festgelegt werden. [6]

Rapid Elasticity: Die verschiedenen Services, welche durch den Service Provider in der Cloud zur Verfügung gestellt werden, werden in ihrer Verfügbarkeit schnell und elastisch reguliert. Daher, wenn viel Rechenressourcen benötigt werden, so werden auch viele bereitgestellt. Aus Sicht der Anwender erscheinen die verschiedenen Ressourcen somit unendlich. [6]

Measured Services: Die Nutzung der verschiedenen Rechenressourcen kann gemessen und somit überwacht und optimiert werden, je nach Auslastung der einzelnen Rechen-ressourcen. Dies kann sowohl von der Seite der Service Provider als auch von der Seite der Anwender geschehen und sorgt so für Transparenz. [6]

Darüber hinaus gibt es noch weitere Eigenschaften, welche Cloud Services in der Regel besitzen. So stellt die Cloud Security Alliance (CSA) etwa das sogenannte “*Measured Pay Per Use*” als Eigenschaft der Cloud vor. Grundlegend beschreibt diese Eigenschaft, dass der Kunde des Cloud Services lediglich für die Ressourcen bezahlen muss, welche er tatsächlich verwendet. Diese Eigenschaft beruht auf der des oben aufgeführten „Measured Services“ wo sowohl der Kunde als auch der Anbieter des Cloud Services in der Lage ist, die Auslastung der Ressourcen zu betrachten und aufzuzeichnen. [7]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat basierend auf den aufgezählten Eigenschaften der Cloud eine eigene Definition des Begriffes erarbeitet. Laut dem BSI handelt es sich bei Cloud Computing, oder der Cloud, um das Anbieten, Nutzen sowie Abrechnen von IT-Dienstleistungen, welche über ein Netz zur Verfügung gestellt werden. Diese werden dabei dynamisch, je nach Bedarf der Nutzer angepasst. Das Anbieten und Nutzen der verschiedenen IT-Dienstleistungen erfolgt dabei über eigens dafür definierte Schnittstellen und Protokollen. Das Angebot von Cloud Services umfasst dabei alle Dienstleistungen, welche das Informationstechnische Spektrum bietet. Dies beinhaltet unter anderem Teile der Infrastruktur, etwa Speicherplatz oder Rechenleistung, aber auch verschiedene Plattformen und Software. [4]

2.1.2 Servicemodelle einer Cloud

Bei der praktischen Anwendung von Cloud Services wird zwischen drei verschiedenen Servicemodellen unterschieden. Die Abgrenzung zwischen diesen Modellen ist dabei nicht absoluter Natur. Somit gibt es teilweise eine Überschneidung der einzelnen Servicemodelle. Ein Servicemodell bezeichnet hierbei eine Beschreibung über den Service als solches, sowie über die enthaltenen Komponenten, welche zur Erfüllung der Aufgaben der Service notwendig sind. [8p.9f]

Die verschiedenen Servicemodelle heißen dabei Software as a Service, Platform as a Service und Infrastructure as a Service. Je nach Modell wird dabei ein Service, also eine Dienstleistung angeboten, welche der Kunde gegen eine Zahlung nutzen kann. [9p.5f]

Bei “Software as a Service” wird es dem Cloud Kunden ermöglicht, die Software des Service Providers, hier des Cloud Anbieters, in der Cloud zu nutzen. Dabei ist die Nutzung geräteunabhängig über einen Webbrowser möglich. In diesem Fall ist die einzige Voraussetzung zur Nutzung der Dienste das Anmelden des Nutzers in der entsprechenden Cloud [10p.55]. Des Weiteren ist das Nutzen der gestellten Software auch über eine installierte Applikation möglich. Wichtig anzumerken ist, dass der Cloud Kunde keinerlei Kontrolle über die Infrastruktur der Cloud hat, beispielsweise über Einstellungen für die Server oder Betriebssysteme. [6]

Als weiteres Servicemodell steht “Platform as a Serivce” zur Verfügung. Hier ist es dem Cloud Kunden möglich entweder „gekaufte“ Software oder selbst programmierte Software auf der Cloud Infrastruktur einzusetzen. Für gewöhnlich wird neben dem Zugriff auf die Infrastruktur auch jegliche Voraussetzungen für eine Programmierumgebung geschaffen, welche beispielsweise Python unterstützt [10p.52]. Dies ermöglicht unter anderem die Entwicklung, Anpassung und Optimierung von eigens programmierter Software [11]. Wie auch schon bei „Software as a Service“ ist es dem Cloud Kunden nicht möglich die Infrastruktur

zu verändern. Er hat jedoch die Kontrolle darüber, welche Software in der Cloud eingesetzt wird [6].

Das dritte Servicemodell, welches im Cloud Computing angeboten und eingesetzt werden kann, ist „Infrastructure as a Service“. In diesem Modell kann der Cloud Kunde auf IT-Ressourcen, wie etwa Rechenleistung, Speicherplatz oder Netzwerke zugreifen, welche vom Serviceprovider gestellt werden. In diesem Modell hat der Cloud Kunde Kontrolle über etwa Betriebssysteme, Speicher und die eingesetzte Software in der Cloud. Einfluss über die einzelnen Hardwarekomponenten, welche die Cloud hosten, hat der Cloud Kunde jedoch auch hier nicht. Diese Kompetenz liegt auch hier vollständig beim Service Provider. [6]

2.1.3 Bereitstellungsmöglichkeiten einer Cloud

Neben den verschiedenen Servicemodellen des Cloud Computing gibt es ebenfalls unterschiedliche Möglichkeiten die Cloud in Unternehmen oder Organisationen zu implementieren, sogenannte Bereitstellungsmöglichkeiten. Laut NIST gibt es dafür 4 Varianten, wobei diese nicht das komplette Spektrum an Cloud Angeboten abdecken. [6]

Die erste Variante, um eine Cloud bereitzustellen ist die sogenannte „Public Cloud“. Sie entspricht der klassischen Vorstellung der Cloud bei welchem Zugriff auf IT-Ressourcen über das Internet durch Webservices oder Webapplikationen zur Verfügung gestellt werden. Die Bereitstellung dieser Ressourcen kann durch ein Unternehmen, einer Regierungsinstitution, durch eine Lehranstalt oder durch eine Kombination zwischen den einzelnen Organisationen erfolgen [9p.6]. Die Cloud wird auf der Hardware des Cloud Anbieters gehostet. Die Services, welche dabei zur Verfügung gestellt werden, können von einer großen Gruppe, beispielsweise der Industriebranche oder von der ganzen Allgemeinheit benutzt werden [6].

Das Gegenstück zur „Public Cloud“ ist die „Private Cloud“. Die große Differenz im Vergleich zu der „Public Cloud“ Variante ist, dass die Dienste, welche in der „Private Cloud“ angeboten werden, exklusiv von einem einzigen Unternehmen verwendet werden. Dabei ist es möglich, dass diese Cloud von Unternehmen selbst geführt, organisiert und kontrolliert wird oder dass diese Aufgabe ein drittes Unternehmen übernimmt. Eine Kombination aus dritten und eigenen Unternehmen ist dahingehend ebenfalls denkbar und möglich. Ein Hosten dieser Cloud ist sowohl von der Hardware des Unternehmens oder auf der eines Dritten möglich. [6]

Eine weitere Möglichkeit, die besteht, um die Dienste einer Cloud anzubieten ist die „Community Cloud“. Bei dieser Variante werden die Dienste der Cloud einer Gruppe von Unternehmen zur Verfügung gestellt, welche die gleichen Neigungen besitzen. Diese Interessen können dabei von Sicherheitsbedenken bis zu Rechtsverordnungen reichen. Die Kontrolle und Ausführung der Cloud geschieht entweder durch eine der Gruppe angehörenden Organisationen oder durch mehre Organisationen der Interessensgruppe. Eine weitere Möglichkeit wäre die Bereitstellung und Wartung der Cloud durch einen Dritten. Eine

Kombination aus dritten und Unternehmen der Gruppe zum gemeinsamen Kontrollieren der Cloud ist ebenfalls möglich. Das Hosten der Cloud ist hier durch die Organisationen selbst oder durch den dritten möglich. [6]

Die Kombination von verschiedenen Bereitstellungsmöglichkeiten nennt man „Hybrid Cloud“ [8p.12]. Dabei werden zwei oder mehr der oben definierten Cloud Bereitstellungsmöglichkeiten (Public, Private, Community) zusammengeführt. Dabei bleiben die einzelnen Varianten als solche bestehen, die Zusammenführung erfolgt dabei über standardisierte Technologie, welche es erlaubt Applikationen und Daten zwischen den Clouds zu transportieren [6].

2.1.4 Die M365 Cloud

Microsoft 365, früher bekannt als Office 365, bezeichnet einen Begriff, hinter denen sich verschiedene Tools verbergen welche in einer Cloud von Microsoft nutzbar sind, im Folgenden wird hier von der M365 Cloud gesprochen. [12]

Die M365 Cloud beinhaltet dabei verschiedene Tools von Microsoft. So sind grundsätzlich immer Word, PowerPoint und Excel in dem Angebot vorhanden aber auch Applikationen wie Teams, Outlook und OneDrive sind enthalten [13]. Im Grundsatz bietet Microsoft mit und in der M365 Cloud „Software as a Service“ an [9p.5]. Dabei gibt es neben diesen Applikationen ebenfalls verschiedene Verwaltungscenter, so z.B.: das Admin- oder das Compliancecenter, in welchen es möglich ist, die Cloud und somit beispielsweise die Nutzerkonten zu verwalten. [14]

Das Angebot der Software der M365 Cloud ist dabei stark an den Kunden angepasst. So gibt es Angebote für Privatkunden, mittelständische Unternehmen, Großunternehmen oder für Schule und Studium [13]. Der große Unterschied in diesen verschiedenen Angeboten, sind die zusätzlichen Applikationen und Inhalte, welche enthalten sind. Beispielsweise hat ein Angebot für Unternehmen, von Microsoft werden diese Angebote „Plan“ genannt, mehr Inhalte und Extras als ein Angebot für Privatkunden [15]. Dabei gibt es auch noch eine weitere Unterscheidung innerhalb der einzelnen Kategorien. So gibt es beispielsweise mehrere Pläne für Großunternehmen, wie auch für jede der anderen Kategorien. Der Unterschied hierbei ist ebenfalls eine andersartige Verteilung von Software und Programmen. In der Regel verhält es sich so, dass durch einen finanziellen Mehraufwand mehr Applikationen zur Verwendung bereitstehen. Dazu gibt es auch mehr Werkzeuge welche zur Verwaltung, Untersuchung der Cloud oder zum Schutz der Informationen durch diesen Mehraufwand verwendet werden können. [16]

Die Bereitstellung des Cloud Service folgt dabei dem Vorbild einer „Public Cloud“. Die Dienste der M365 Cloud werden mehreren, um nicht zu sagen allen, interessierten Organisationen angeboten. Diese besitzen teilweise stark unterschiedlich gelagerte Zielsetzungen und Aufgabengebiete und können nicht zu einer einzelnen Interessensgemeinschaft zusammengefasst werden. [11]

2.2 Das Tool eDiscovery

Innerhalb der M365 Cloud stehen verschiedene Werkzeuge zur Verfügung, welche unter anderem das Verwalten und die Aufgaben innerhalb der Cloud erleichtern sollen. Das Werkzeug eDiscovery gehört ebenfalls dazu und soll im Folgenden erläutert werden, um so eine Grundlage für die spätere Beantwortung der Fragestellung zu schaffen. [3]

2.2.1 Begriffserklärung eDiscovery

Hinter dem Begriff „eDiscovery“ verbirgt sich ein Prozess, welcher in seinem ursprünglichen Begriff darauf hinausläuft, elektronische Daten zu durchsuchen, zu lokalisieren und schlussendlich zu speichern und sicher aufzubewahren. Diese sollen anschließend als Beweis in einem Straf- oder Zivilprozess vor Gericht verwendet werden. Diese Untersuchung kann dabei beispielsweise von der Regierung oder durch ein Gericht angeordnet werden, je nach den jeweiligen Regelungen in den einzelnen Ländern [17]. Es ist ebenfalls möglich, dass eDiscovery als Teil einer internen Untersuchung verwendet wird. Der Prozess eDiscovery bezieht sich aber hauptsächlich auf digitale Beweise, wie E-Mails, Online-Dokumente oder Datenbanken [18]. In der Regel ist eDiscovery damit Teil einer größeren Untersuchung zur Wahrheitsfindung und kann dahingehend als Werkzeug zu ebenjenem Ziel betrachtet werden.

Das Ziel von eDiscovery ist es im Zuge des Suchens, Lokalisieren und dem Speichern der Daten, die 5 W-Fragen zu beantworten. Bei diesen W-Fragen handelt es sich um „Wer“, „Was“, „Wann“, „Wo“ und „Warum“. Essenziell ist somit beim eDiscovery Prozess herauszufinden, welche Person bzw. Nutzer auf welches Dokument oder E-Mail, zu welchem Zeitpunkt zugegriffen hat. Dabei soll ebenfalls herausgefunden werden wo das Dokument innerhalb der Cloud gespeichert ist und warum auf das Dokument zugegriffen wurde, beispielsweise zur Bearbeitung oder zur Weiterverbreitung. Das „Warum“ ist dabei stark abhängig von dem Verständnis der Untersuchenden hinsichtlich der Gegebenheiten des Falles und seiner Eigenschaften. [19p.60]

Grundlage für jegliche Suche mithilfe von eDiscovery ist eine große Menge verschiedener Dokumente, welche durchsucht werden können. Gibt es diese nicht ist eine eDiscovery Suche überflüssig. In den meisten heutigen Clouds, welche Unternehmen benutzen, entstehen allerdings sehr schnell solche Datenmengen, welche für ein manuelles Durchsuchen zu groß sind. Allgemein bedient sich der Prozess eDiscovery zwei Prozessen, namentlich

„Information retrieval“ und „Information extraction“ um die Untersuchung der Datenmenge durchzuführen.[20]

Durch Methoden der “Information extraction” wird dabei die Suche so angepasst, dass Ergebnisse, welche durch eDiscovery gefunden werden, relevanter für den Fall sind, welcher betrachtet wird. Mögliche verwendete Methoden sind zum Beispiel das Extrahieren von Entitäten, das Identifizieren von Beziehungen zwischen einzelnen Dokumenten oder das Herausfinden der Themen in den einzelnen Dokumenten. Jede dieser Methoden ermöglicht es eDiscovery mehr Informationen zu finden und zu identifizieren. Durch „Information retrieval“ ist es anschließend möglich, die gefundenen Informationen zu extrahieren und zusammenzufassen. [20]

Der Prozess eDiscovery kann dabei auf verschiedene Art und Weise angesehen werden, welche die weitere Arbeitsweise und Methodik beeinflussen.

Zum einen gibt es die Annahme, dass das eDiscovery Ziel nicht von Beginn an feststeht und dass das Wissen, und somit die relevanten Dokumente erst mit fortschreitender Zeit und mehreren Suchen gefunden werden. Die Suche wird hier erforschend eingesetzt und damit einhergehend werden die Suchparameter stetig ergänzt, um so nach und nach ein möglichst präzises und zutreffendes Ergebnis zu erhalten, daher möglichst viele relevante Dateien zu finden. [19p.62]

Eine andere Art eDiscovery zu betrachten, besteht darin, dass der eDiscovery Prozess eine Suche nach der Nadel im Heuhaufen ist und daher das Ziel an sich bereits bekannt ist. Die Nadel sei dabei die, verhältnismäßig wenigen, relevanten Dateien im Heuhaufen, welche alle Daten in der Organisation darstellt. [19p.62]

Bei eDiscovery liegt der Fokus der Suche dabei auf einem hohen Recall, welcher somit gegen 100% gehen sollte. Das heißt möglichst alle wesentlichen Daten, welche die Suchbegriffe enthalten, sollen gefunden werden, auch wenn ihre tatsächliche Relevanz am Ende für die Untersuchung gering ist. [19p.62]

Der eDiscovery Prozess ist dabei bei jeder Durchführung unterschiedlich und somit einmalig [19p.62]. Jede Untersuchung birgt dabei unterschiedliche Herausforderungen. Diese Herausforderungen, welche vor allem die Dauer eines eDiscovery Prozesses bestimmen, sind beispielsweise die Größe des Korpus in welchem alle zu durchsuchenden Dokumente zusammengefasst sind. Ein weiterer Punkt, der zum Tragen kommen könnte, ist die Verfügbarkeit der Dokumente. So ist es, abhängig von der Organisation, nicht gewährleistet, dass unverzüglich alle Dokumente zur Untersuchung bereitstehen. Ein anderer Umstand, welcher die Verwendung von eDiscovery einschränken könnte, ist die Unterschiedlichkeit der Dokumententypen. Für den Großteil der gängigen Dokumententypen müssen in

eDiscovery Funktionen implementiert sein um diese durchsuchen und überprüfen zu können [21]. Darüber hinaus muss es möglich sein, die relevanten Daten in einem gängigen Format wie etwa PDF darzustellen.[22]

Bei der forensischen Nutzung von eDiscovery ist es in der Regel erforderlich, dass alle zur Verfügung stehenden Werkzeuge und Methoden verwendet werden, beispielsweise verwandte Prozesse wie der Audit Log oder andere Analyse Werkzeuge, um so einen möglichst umfassenden Bericht zu erstellen und einen Großteil aller zur Verfügung stehenden Daten zu durchsuchen und zu sichern. Dazu gehören beispielsweise auch Werkzeuge oder implementierte Funktionen, welche gelöschte Daten wieder herstellen können. Dabei sei jedoch erwähnt, dass unter bestimmten Umständen, wie etwa Zeitdruck oder fehlenden technischen Ressourcen bestimmte Methoden nicht möglich ist. Eine andere, sehr wichtige Komponente bei der Arbeit mit dem Prozess eDiscovery ist die Kontrolle und damit einhergehende Dokumentation, welche Person wann mit den einzelnen Werkzeugen arbeitet und wer wann auf Daten zugegriffen hat. Einhergehend mit dem letzten Punkt muss dabei ein Konzept bestehen welche Personen berechtigt sind auf die Daten zuzugreifen oder die Werkzeuge zu verwenden. Ist dies nicht der Fall so ist die Integrität der Daten gefährdet und die Ergebnisse können unter Umständen nicht verwendet werden. [19p.63]

2.2.2 Das Electronic Discovery Reference Model

Ein einheitlicher Vorgang für die Verwendung eines eDiscovery Prozesses existiert dabei nicht. Je nach Anbieter der eDiscovery Software ist auch der Prozess eDiscovery unterschiedlich und damit einzigartig. Eine mögliche Orientierung über den Ablauf eines eDiscovery Prozesses bietet das Electronic Discovery Reference Model (EDRM) wie in Abbildung 1 gezeigt. Dies ist dabei lediglich ein Konzept für eDiscovery Prozesse und kein starres Model, dem unter jedem Umstand gefolgt werden muss. Je nach unterschiedlichem eDiscovery Prozess werden einzelne Punkte nicht ausgeführt oder Punkte werden, sollte es erforderlich sein, mehr als einmal im Prozess verwendet. Jede einzelne Phase gibt darüber hinaus Feedback um den eDiscovery Prozess für weitere Einsätze zu optimieren. [23]

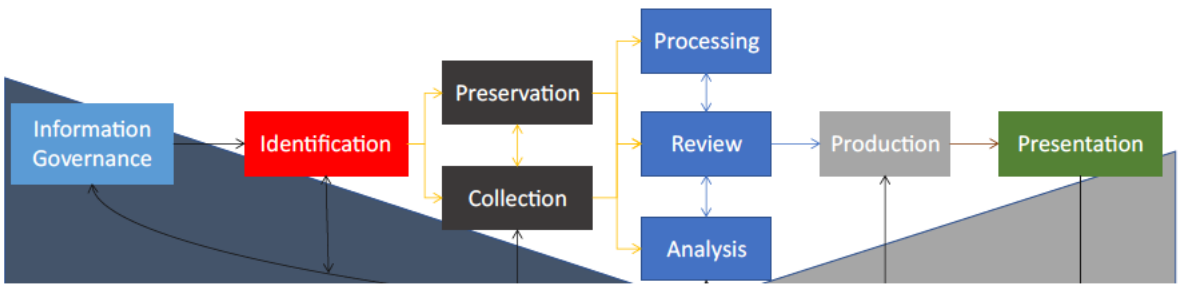


Abbildung 1: EDRM nach [23]

Die erste Phase des EDRM ist „Information Governance“. Hier wird bestimmt wie die Daten, auch „electronically strored Information“ (ESI) genannt, innerhalb der Organisation ordnungsgemäß gespeichert und verwaltet werden. Es werden dafür verschiedene Abläufe und Richtlinien erstellt. Dies ist dahingehend von Relevanz, wenn dadurch Kosten und Risiken wie beispielsweise Datenschutzverletzungen minimiert werden, sollte der eDiscovery Prozess eingesetzt werden müssen.[24]

Die nächste Phase des EDRM ist die der „Identification“. Das Ziel dieser Phase ist das Aufspüren von potenziell relevanten ESI-Quellen und das Bestimmen ihrer Parameter. Mögliche Quellen sind dabei Personen als solche, IT-Systeme oder ganze Abteilungen einer Organisation. Es geht hier vor allem darum, einen Plan zu entwickeln wie vorgegangen wird, sollte der eDiscovery Prozess eingesetzt werden müssen. Das Wissen darüber, wo welche Daten liegen und wer mit welchen Daten arbeitet, ist hilfreich für eine Suche mit eDiscovery und erleichtert diesen Prozess. Die Phase der „Identication“ sollte so umfassend und gründlich wie möglich geschehen. [25]

Nach der Entwicklung eines Plans zur Identifikation von ESI ist die darauf aufbauende Phase des EDRM „Preservation“. Hier geht es ebenfalls um die Entwicklung eines standardisierten Plans und Vorgehens. Das Hauptziel hierbei ist, dass potenziell relevante ESI geschützt sind gegen Änderung oder Löschung. Dieser Vorgang tritt dabei ein, sobald der eDiscovery Prozess beginnt. Mögliche relevante Daten werden somit isoliert und geschützt. [26]

Nach der Erstellung des Vorgehens zur Sicherung von Daten ist die nächste Phase die der „Collection“. Hier, in dieser Phase, geht es ganz konkret um das Suchen und Sichern von ESI und seinen Metadaten für den weiteren Gebrauch im eDiscovery Prozess. Die Sicherung muss dabei so erfolgen, dass ESI in einem Gerichtsprozess verwendet werden können. So muss beispielsweise glaubhaft dargelegt werden, dass die Daten nicht nachträglich manipuliert wurden und die Suchergebnisse unverändert sind. [27]

Alle Phasen und Arbeitsschritte, welche bis hierhin durchgeführt wurden, dienten dem Aufspüren und Klassifizieren von Daten. Die Verarbeitung der gefundenen Daten beginnt in den nächsten Phasen.

Nach der Sammlung von potenziell relevanten Dokumenten ist die nächste Phase „Processing“ dafür verantwortlich, die gesammelten ESI zu verarbeiten. Dabei gehört beispielsweise das Entfernen von mehrfach vorkommenden ESI aus den gesammelten Dateien durch Hash-Werte (mit welchem jede Datei versehen wird) zu den angewandten Methoden. Ein anderer wichtiger Punkt, welcher beim „Processing“ stattfindet, ist das Entpacken von komprimierten Dateien und damit einhergehend das vollständige Erkunden der entsprechenden Daten. Des Weiteren ist es möglich, dass aus (verschlüsselten) Dateien Texte und

Metadaten extrahiert werden. Ebenfalls eine mögliche Option in dieser Phase ist die Tokenisierung von Dateien, um so eine Datenbank zu bilden. Genauso ist das Sortieren von Dateien nach Datum, Dateityp oder eine andere Variable ein Mittel, um die bisherigen Ergebnisse einer eDiscovery Suche zu verarbeiten und zu ordnen. [28]

Nachdem ESI verarbeitet wurde, folgt die nächste Phase des EDRM, die „Review“ Phase. Hier wird die jetzt verarbeiteten ESI nach ihrer Relevanz bewertet. Allgemein ist das Ziel dieser Phase, ein Verständnis von dem Inhalt der Dokumente zu bekommen und so eine fundierte Bewertung der Dokumente nach Relevanz durchzuführen und so am Ende faktisch irrelevante Dokumente auszusortieren. Dabei kann es eine Option sein, zusammenhängende Dokumente gemeinsam zu betrachten, um so ein effizienteres Arbeiten zu ermöglichen und Kosten zu sparen. [29]

Die nächste, ähnlich klingende Phase ist die der „Analysis“. Dabei werden auch, wie in der „Review“ Phase die gefundenen Dokumente betrachtet. Hauptpunkt dieser Phase ist das Verstehen der Fakten und Informationen innerhalb der relevanten Dokumente, um so Muster und Zusammenhänge für einen möglichen Gerichtsprozess zu erkennen. Ein weiterer Vorgang, welcher in „Analysis“ vonstattengeht, ist die Verbesserung der Suchbedingungen für die aktuelle, aber auch für weitere Suchen. Dabei werden verschiedene Rollen mit unterschiedlichen Aufgaben erstellt und verteilt, um so den gesamten Prozess möglichst effizient zu gestalten und alle Aufgaben an geschulte Personen zu vergeben. Sollte der eDiscovery Prozess zum ersten Mal durchgeführt werden, muss im Vorhinein geklärt werden, welche Person die einzelnen Phasen bearbeitet. Je nach auftretenden Problemen kann so beim nächsten Mal der Zeitplan und das Personal angepasst werden. Ein weiterer Punkt ist die Verbesserung der „Review“ Phase. Dabei geht es vor allem um das Erfassen der Zeit, die benötigt wird, um die Dokumente in der „Review“ Phase zu bewerten. Ein anderer wichtiger Punkt ist die Bewertung der Arbeit der Reviewer. Hier ist das doppelte Bewerten einer Datei eine zielführende Methode, um die Qualität der Reviewer zu bestimmen. Damit einhergehend ist ein ebenfalls wichtiger Punkt der „Analysis“ Phase, nämlich die Validierung der Ergebnisse und Erkenntnisse. Diese Gewährleistet die Qualität der Arbeit der „Analysis“ Phase für den Gerichtsprozess. Dazu gehört etwa die Erstellung einer Dokumentation, welche zeitgleich zum Arbeitsprozess erstellt wird und alle Arbeitsschritte und auftretende Probleme enthält. [30]

Die vorletzte Phase des EDRM ist die Phase der „Production“. Hier geht es vor allem darum, die bisher extrahierten, relevanten ESI in lesbare Formate umzuwandeln, sollte dies nicht bereits der Fall sein. Dies ist notwendig, um sie anderen zukommen zu lassen und somit beispielsweise ihre Verwendbarkeit vor Gericht zu gewährleisten. Ebenfalls wird in dieser Phase über eine angebrachte Art und Weise entschieden, wie die relevanten ESI an andere Parteien übermittelt werden. Wichtig ist, dass diese Aufgaben entsprechend den Absprachen zwischen den beiden Parteien bearbeitet werden, um eine reibungslose Verwendung zu gewährleisten. [31]

Die letzte Phase ist die der „Presentation“. In dieser Phase werden die verarbeiteten, relevanten ESI vor der jeweiligen Audienz präsentiert, beispielsweise bei einem Gerichtsprozess. Die Dateien werden dabei in der Regel in ihrem ursprünglichen Format gezeigt oder in einem Format, in welchem möglichst wenig Informationen verloren gehen. Ziel ist es, neue Informationen, welche durch die Untersuchungen des eDiscovery Prozesses ans Licht gekommen sind, zu vermitteln, bestehende Fakten oder Positionen zu untermauern und das Gericht von einem Tathergang zu überzeugen. [32]

Die einzelnen Phasen können dabei, wie bereits erwähnt, in unterschiedlichen Reihen-folgen auftreten oder sich mehrmals wiederholen. Ausschlaggebend dafür ist, wie der eDiscovery Prozess in der Organisation definiert ist. [23]

2.2.3 eDiscovery in der M365 Cloud

Innerhalb der M365 ist eDiscovery abhängig der Lizenz nutzbar. So braucht man auf jeden Fall eine Lizenz für Unternehmen, sollte man die implementierte eDiscovery Lösung von Microsoft in der M365 Cloud nutzen wollen. Dabei unterscheiden sich die Optionen für die Lösung von eDiscovery ebenfalls je nach Lizenz [16]. Es gibt zwei verschiedene Arten von eDiscovery Lösungen in der Cloud, zum einen Standard eDiscovery und zum anderen Premium eDiscovery. Beide bauen auf der Funktion der Inhaltssuche auf, die ebenfalls zur Verwendung bereitsteht [3]. Um die Funktionen der Inhaltssuche zu verwenden, braucht man, genau wie bei der eDiscovery Suche eine Unternehmenslizenz. Die verschiedenen eDiscovery Funktionen stehen mit den Lizenzen E-3 (Standard eDiscovery) und E-5 (Premium eDiscovery) zur Verfügung [16]. Um eDiscovery zu nutzen, muss man zunächst im Compliance Portal von Microsoft angemeldet sein. Dort stehen unter dem Reiter eDiscovery beide eDiscovery Lösungen zur Verfügung, wie in Abbildung 2 dargestellt. Vorausgesetzt, die Lizenz beinhaltet eDiscovery [33].

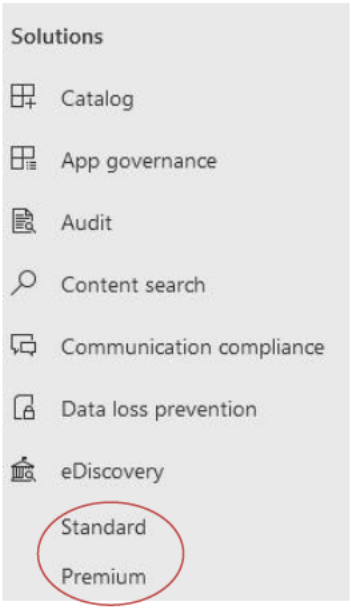


Abbildung 2: Auswahl eDiscovery im Compliancemanager mit E-5 Lizenz

Die Suche beider eDiscovery Lösungen findet dabei standardmäßig in den Applikationen und Speicherorten statt, welche durch die M365 Cloud für den Endnutzer bereitstehen. Genauer formuliert durchsucht eine Abfrage in eDiscovery alle Inhalte, welche in OneDrive for Buisness, SharePoint Online, Exchange Online, Microsoft Teams, Microsoft 365 Gruppen und Yammer Teams gespeichert sind [3]. Dabei ist es möglich in einer Suche gleichzeitig sowohl Mailboxen als auch Speicherorte wie SharePoint Online zu

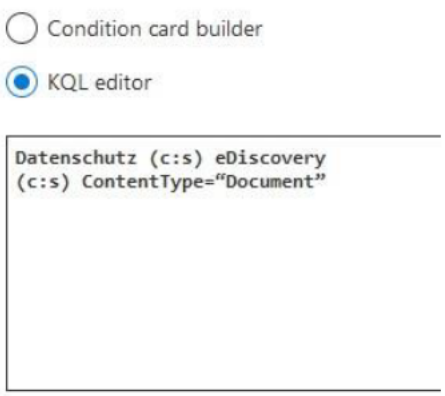
durchsuchen und zu identifizieren. Anschließend ist es möglich, die Suchergebnisse zu speichern und sie zu exportieren [34].

Die Gemeinsamkeit der beiden eDiscovery Lösungen neben der Möglichkeit des Exports von Suchergebnissen ist die gezielte Fallverwaltung durch eDiscovery. Dabei ist es möglich, dass eDiscovery Suchen bestimmten Fällen zugeordnet werden. Dadurch ist machbar zu kontrollieren, wer Zugriff auf die Suchfunktion sowie die Suchergebnisse besitzt. Ebenfalls werden Suchergebnisse bei beiden eDiscovery Lösungen so gespeichert, dass sie vor Gericht verwendet werden können. Hier wird der versehentlichen oder bewussten Löschung von Inhalten vorgegriffen. Durch die redundante Speicherung der Daten werden die Inhalte ebenfalls gegen Manipulation geschützt [3].

Die Unterschiede der beiden eDiscovery Lösungen liegen vor allem im Bereich der Analyse der Suchergebnisse. Hier bietet Premium eDiscovery eine sehr große Auswahl an verschiedenen Funktionen, welche die Betrachtung und Auswertung der Suchergebnisse stark vereinfachen. Die Möglichkeiten sind in Standard eDiscovery allesamt nicht enthalten. Eine Funktion, welche die Verarbeitung in Premium eDiscovery erleichtern, sind beispielsweise die sogenannte „Fehlerbehebung“. Diese ermöglicht es, dass beispielsweise kennwortgeschützte Dateien in der eDiscovery Suche betrachtet werden können. Ebenfalls wird als Funktion die optische Zeichenerkennung angeboten. Dadurch ist es möglich Texte aus Bilddateien zu erkennen. Das Bild mit dazugehörigen Text kann anschließend in einen Fall inkludiert werden. Darüber hinaus gibt es verschiedene Möglichkeiten, sehr gleiche Dateien zu erkennen und diese dementsprechend zu gruppieren. [3]

Die Suche der beiden eDiscovery Varianten beruht, wie bereits erwähnt auf der implementierten Inhaltssuche innerhalb der M365 Cloud. Diese Inhaltssuche erlaubt zunächst auszuwählen, welche Speicherorte durchsucht werden können. Zur Auswahl stehen hierbei Exchange Mailboxen, SharePoint Sites oder Exchange Public Folders. Ebenfalls können noch in Teams nach Chatdaten gesucht werden. Sollte eines der eben aufgeführten Orte nicht als Suchgebiet ausgewählt werden, so werden auch keine Inhalte gefunden, welche dort gespeichert sind. [35]

Die Suchbegriffe können dabei als einzelne Stichwörter eingegeben werden beziehungsweise sollten mehrere Wörter oder Ausdrücke als Suchbegriffe eingegeben werden, so werden diese standardmäßig mit einem „OR“ Operator in der Suche miteinander verknüpft. Dieser wird in der eDiscovery Suche als „(c:s)“ dargestellt, wie in Abbildung 3 zu sehen ist [34]. Darüber hinaus kann man eine genauere Suche durchführen, indem man verschiedene Kriterien einfügt. Das können beispielsweise das Sende- oder Empfängerdatum oder der letzte Änderungszeitpunkt einer



0 **Abbildung 3: eDiscovery Suche**

Datei sein. Darüber hinaus ist es auch möglich, nach dem Dokumententyp zu filtern, etwa nach Dokumenten oder Videos. [36]

Je nach Suchanforderung ist es dabei möglich, die verschiedenen Kriterien und Einschränkungen mithilfe von booleschen Operatoren zu verknüpfen und so komplexe Abfragen zu erstellen. Zur Verfügung stehen dabei die Operatoren „AND“, „OR“, „NOT“ sowie „NEAR“. Mit diesen ist es möglich, Suchanfragen genauer zu gestalten. Wird keiner dieser Operatoren verwendet und lediglich Suchbegriffe eingegeben, so werden diese automatisch mit einem logischen „OR“ verknüpft [35]. Gibt man beispielsweise die Suchbegriffe „eDiscovery“ und „Datenschutz“ ein, wird nach Dokumenten gesucht, welche entweder den Begriff „eDiscovery“, den Begriff „Datenschutz“ oder beide Begriffe beinhalten. Nach dem Durchführen der Suche werden zunächst die Anzahl der Speicherorte sowie eine geschätzte Anzahl an Suchergebnissen angezeigt. Diese Darstellung ermöglicht einen schnellen Überblick [37]. Des Weiteren ist ebenfalls das Anzeigen einer Statistik, welche die Inhaltsspeicherorte der gefundenen Elemente darstellt, möglich. Darüber hinaus ist es nach der Suchanfrage umsetzbar, eine Vorschau der Ergebnisse angezeigt zu bekommen und diese Vorschau lokal zu exportieren [38].

Das Werkzeug eDiscovery in der M365 Cloud ist dabei nicht mit dem kompletten Prozess eDiscovery zu verwechseln und gleichzusetzen, welchen das EDRM darstellt. Es kann jedoch sehr wohl in die Phasen ebenjenes eingeordnet werden. So umfasst das Werkzeug eDiscovery die Phase „Collection“ komplett, ferner werden die Phasen des „Processing“, der „Review“ sowie der „Analysis“ teilweise von diesem Werkzeug erfasst und bearbeitet. Andere Phasen wie „Identification“ oder „Presentation“ werden nicht erfasst. Somit bietet eDiscovery in der M365 Cloud als Werkzeug bereits verschiedene Funktionen, um den weiteren eDiscovery Prozess zu unterstützen.

2.2.4 Nutzer des Werkzeugs eDiscovery in der M365 Cloud

Die verschiedenen Varianten von eDiscovery, sowohl Standard als auch Premium eDiscovery, können standardmäßig von niemandem verwendet werden. Um als Nutzer die Funktionen von eDiscovery zu verwenden, ist es nötig, dass die entsprechende Berechtigung zur Verwendung dem jeweiligen Nutzer zugewiesen wird. [39]

Die notwendigen Berechtigungen werden dabei im Complianceportal von Microsoft vergeben. Eine Übersicht einer Berechtigungsgruppe ist dabei in der Abbildung 4 zu sehen. [40]

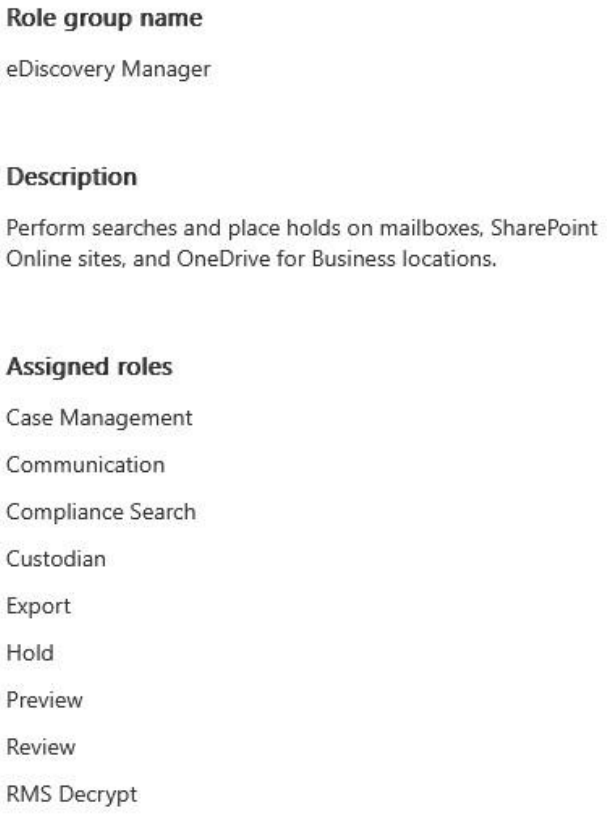


Abbildung 4: Übersicht über eDiscovery Manager Rolle

Die Berechtigungen können beispielsweise von einem globalen Administrator vergeben werden. Welche Person innerhalb der Organisation für die Nutzung von eDiscovery berechtigt und geschult ist, muss intern geklärt werden. Es gibt dabei standardmäßig zwei verschiedene, bereits von Microsoft vorkonfigurierte Rollen, welche Nutzern zugewiesen werden können, die es ermöglichen, eDiscovery zu verwenden. Zum einen ist es die Rolle des „eDiscovery Managers“. Diese Rolle erlaubt es dem Nutzer, einen eDiscovery Fall zu erstellen und in ihm Suchen durchzuführen. Des Weiteren kann er diese Suchen bearbeiten und die Inhalte aus den Suchergebnissen exportieren. Darüber hinaus wird durch diese Berechtigungen der Nutzer befähigt, andere Nutzer als Mitglieder zu dem Fall hinzuzufügen

sowie diese wieder zu entfernen. Diese Nutzer haben dann nur beschränkte Möglichkeiten in dem Fall und können beispielsweise lediglich Dokumente nach ihrer Relevanz bewerten. Anzumerken ist hierbei, dass ein „eDiscovery Manager“ nur auf die eDiscovery Fälle zugreifen kann, welche er selbst erstellt hat oder zu denen er von anderen Managern aktiv hinzugefügt wurde.

Die andere Rolle, die den Nutzer dazu befähigt, eDiscovery zu verwenden, ist die des „eDiscovery Administrators“. Dieser besitzt alle Berechtigungen und Möglichkeiten, welcher ein „eDiscovery Manager“ besitzt. Darüber hinaus kann ein „eDiscovery Administrator“ auf jegliche eDiscovery Fälle zugreifen, welche in der jeweiligen M365 Cloud aktiv sind und ausgeführt werden. Damit einhergehend kann er zum einem auf jegliche Suche und die dazugehörigen Suchergebnisse zugreifen und diese exportieren. Des Weiteren ist der Administrator dazu befähigt, „eDiscovery Manager“ aus einem Fall zu entfernen, selbst wenn diese den Fall erstellt haben [40].

Microsoft empfiehlt, dass nicht viele Nutzer die Rolle des „eDiscovery Administrator“ zugewiesen bekommen. Dies könnte die Integrität des Prozesses eDiscovery stören und negativ beeinflussen. Der Großteil der eDiscovery Verwendung sollte somit von „eDiscovery Managern“ durchgeführt werden, welche nur Zugriff auf die von ihnen erstellten Fälle besitzen. Generell sollten laut der Microsoft Dokumentation, lediglich bereits bestehende Administratoren auch „eDiscovery Administrator“ werden. Empfehlenswert ist dieses Vorgehen ebenfalls für die Vergabe des „eDiscovery Managers“. Es ist dabei ebenfalls möglich, die bereits bestehenden, vorkonfigurierten Rollen von Microsoft zu kopieren und zu bearbeiten, um so die Rechte und Möglichkeiten beider Rollen zu erweitern oder einzuschränken. [40]

2.2.5 Verwendungsgebiete von eDiscovery

In seiner ursprünglichsten Form ist das Suchwerkzeug eDiscovery und auch der Prozess eDiscovery als Mittel zur Unterstützung forensischer Ermittlungen anzusehen. Das bedeutet, dass eDiscovery eingesetzt wird, um Daten zu finden, zu sichern und zu extrahieren.

Dieser juristische Ernstfall im Straf- oder Zivilverfahren kann auf zwei unterschiedliche Arten eintreten. Zum einen kann das Unternehmen im Zuge eines Strafverfahrens oder Rechtsstreitigkeit dazu aufgefordert werden, diese Daten an das Gericht zu übermitteln. Dabei kann die Organisation direkt am Prozess beteiligt sein oder als dritter dazu aufgefordert werden. Der Prozess eDiscovery kann verwendet werden, um diese Daten aufzuspüren und sicher zu verwahren, sodass sie innerhalb des Prozesses verwendet werden können. Dabei ist es ebenfalls möglich, dass die Organisation von sich aus beschließt, eDiscovery zu benutzen, um so bereits bei Prozessbeginn in der Lage ist, verschiedene Beweise

vorzulegen und ihren Standpunkt zu untermauern. Hierbei gibt es keinen Beschluss oder Ähnliches eines Gerichts, sondern lediglich den Willen der Organisation. [18]

Neben der Verwendung von eDiscovery als Mittel im juristischen Ernstfall ist es ebenfalls naheliegend, den Prozess eDiscovery und die damit verbundenen Mittel in internen Untersuchungen einzusetzen. Dabei ist das Spektrum, welche interne Untersuchungen umfassen breit gefächert. So können interne Untersuchungen notwendig sein, wenn sensible Daten der Organisation an die Außenwelt gelangen und so die Reputation oder den Gewinn der Organisation schädigen. Sollte diese Situation eintreten, kann eDiscovery eingesetzt werden, um herauszufinden, welche Personen innerhalb des Unternehmens Zugriff auf die veröffentlichten Daten hatten und diese weitergeleitet haben könnten. Des Weiteren kann durch diese Anwendung von eDiscovery mögliche Sicherheitslücken aufgespürt werden, welche im Nachhinein geschlossen werden können. Auf der anderen Seite des Spektrums ist die Ermittlung bezüglich einer Beschwerde innerhalb der Organisation. Diese kann von Mobbing einer Person bis hin zu Diskriminierung und rassistischem Handeln reichen. Um diese Aktionen und Ausdrücke nachzuweisen, kann eDiscovery verwendet werden. Vorausgesetzt diese Anfeindungen geschehen in unserem Fall in der M365 Cloud. [41]

Abgesehen von internen Untersuchungen und juristischen Prozessen ist eine weitere Verwendungsmöglichkeit von eDiscovery die Bearbeitung von Datenschutzanfragen. Innerhalb der Europäischen Union haben die Bürger ein Recht zu erfahren, was die Unternehmen mit ihren Daten machen und welche ihrer Daten sie gespeichert haben. [42 p.119/40f]. Um dies von den jeweiligen Organisationen zu erfahren, sind diese verpflichtet, eine umfassende Antwort zu leisten. Diese beinhaltet alle Dokumente und E-Mails, welche die Daten des Anfragenden enthalten. Sollten diese beispielsweise in der M365 Cloud gespeichert sein, ist es durch eDiscovery möglich, sie aufzuspüren und zu extrahieren. Im Anschluss ist es möglich, diese zu bearbeiten und an den Anfragenden weiterzuleiten.

2.3 Kontrolle und Einschränkung von eDiscovery in der M365 Cloud

Aufgrund der Möglichkeit von eDiscovery, überall in der M365 Cloud nach Inhalten zu suchen, ist eine Kontrolle und damit verbundene Einschränkung notwendig. Dabei ist zu unterscheiden, ob man durch technische Optionen die Funktion von eDiscovery einschränkt oder ob man durch organisationsinterne Prozesse im Nachhinein überprüfen kann, welche Person eDiscovery verwendet hat und welche Dateien mithilfe des Tools betrachtet wurden.

2.3.1 PowerShell

Eine Möglichkeit zur Einschränkung der Funktionsweise von eDiscovery ist die Nutzung von Windows PowerShell und das damit verbundene Erstellen von Filtern für eDiscovery. [44] Eine Shell ist dabei eine Schnittstelle zum Betriebssystem, sie ist somit die äußerste Schicht, welche ein Betriebssystem besitzt. Die Interaktion zwischen Benutzer und Betriebssystem läuft über die Shell und wird von ihr verwaltet. Dies geschieht dadurch, dass die Shell zunächst den Benutzer zur Eingabe eines Befehls auffordert. Dieser Befehl wird nun durch die Shell für das Betriebssystem interpretiert und schlussendlich verarbeitet die Shell die Ausgabe des Betriebssystems. Die Kommunikation zwischen Benutzer und Betriebssystemen über die Shell kann dabei entweder über einzelne Befehle geschehen oder über eine Datei, in welcher Shell- und Betriebssystembefehle gespeichert sind. Im zweiten Fall spricht man von einem Shell-Script. [43]

Die Windows PowerShell ist dabei ein von Microsoft entwickeltes, plattformübergreifendes Framework, welcher zur Konfigurationsverwaltung und Aufgabenautomatisierung verwendet werden kann. Die Ausführung von PowerShell kann dabei über Windows, macOS oder Linux geschehen. Das Framework besteht aus einer Befehlzeilenshell und einer Skriptsprache. Dabei kann Windows PowerShell neben Text auch .NET-Objekte akzeptieren und zurückgeben. Die Skriptsprache der PowerShell basiert auf .NET Common Language Runtime. Über die Windows PowerShell ist es dabei möglich, die Funktionen von eDiscovery durch verschiedene Befehle einzuschränken. [44]

Diese Einschränkung von eDiscovery bzw. genauer gesagt von eDiscovery Managern bezeichnet man dabei laut Microsoft als „Einrichtung von Compliancegrenzen für eDiscovery-Untersuchungen“. Um diese Grenzen einzurichten und Regeln zu definieren, ist es zunächst notwendig, verschiedene Voraussetzungen zu klären, welche in der Cloud gegeben sind. [45]

Gehen wir dabei von einem einer multinationalen Organisation mit Namen „Mittelerde“ aus. Die Organisation besteht aus verschiedenen Tochtergesellschaften, in unserem Beispiel sind das namentlich die Tochtergesellschaften 1 „Auenland“ und die Tochtergesellschaft 2 „Gondor“, wie in Abb. 5 zu sehen.

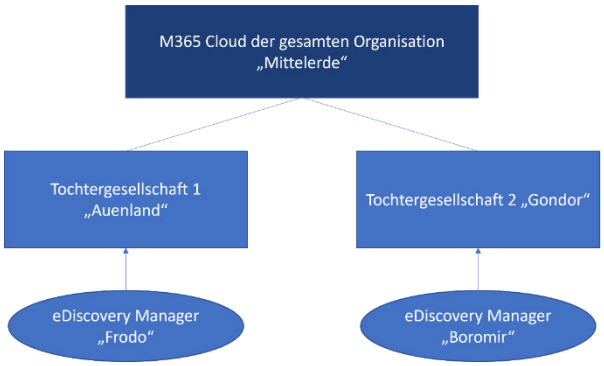


Abbildung 5: Organigramm der Organisation "Mittelerde“

Sollte es nun eine eDiscovery Untersuchung innerhalb der Organisation geben, ist es erforderlich, dass die jeweiligen

eDiscovery Manager lediglich die Daten der jeweiligen Tochtergesellschaft betrachten können. So darf „Frodo“ nur die Inhalte durchsuchen, welche sich im „Auenland“ befinden, nicht jedoch die betrachten, welche in „Gondor“ gespeichert sind. Bei eDiscovery Manager „Boromir“ verhält sich die Sachlage identisch. Betrachten darf er bloß die Daten, die in der zugehörigen Tochtergesellschaft „Gondor“ gespeichert sind. Keinen Zugriff soll er auf die Daten der Tochtergesellschaft „Auenland“ haben. Um dies umzusetzen, ist die Implementierung von Compliancegrenzen notwendig.

Der erste Schritt, um diese Grenzen umzusetzen, ist zunächst das Identifizieren und Auswählen eines Attributes, welche die verschiedenen Tochtergesellschaften definiert. Dies wird benötigt, um anschließend einen Suchberechtigungsfilter für die jeweiligen eDiscovery Manager zu erstellen. In unserem Beispiel wären die Attribute die Namen der beiden Tochtergesellschaften und somit „Auenland“ und „Gondor“. Andere mögliche Attribute, welche in Erstellung von Filtern verwendet werden können, sind der Name verschiedener Abteilungen oder Büros. Es ist auch möglich, die Ländervorwahl als zweistellige Zahl in einem Filter zu implementieren.

Nach dem Auswählen eines Filterattributs ist es ebenfalls notwendig, einen eDiscovery Manager für jede Tochtergesellschaft zu erstellen. Dies liegt darin begründet, dass die verschiedenen Einschränkungen auf die Rolle der eDiscovery Manager angewandt werden und so wirken. Das Erstellen der verschiedenen eDiscovery Manager erfolgt dabei im Compliancecenter. Die einfachste und schnellste Möglichkeit, die neuen „eDiscovery Manager“ zu erstellen, ist es, die bereits bestehende „eDiscovery Manager“ Rolle mit all ihren Rechten zu kopieren und umzubenennen. Sollte man entscheiden, dass bestimmte Berechtigungen innerhalb der Rollengruppe nicht an die Manager vergeben werden sollen, ist es ebenfalls möglich, diese in den Complianceportal zu entfernen. In unserem Fall erstellen wir nun zwei neue eDiscovery Manager Rollen. Zum einen „eDiscovery Manager Frodo“ und zum anderen „eDiscovery Manager Boromir“ auf welche die Compliancegrenzen nun angewandt werden sollen.

Die eigentliche Einschränkung der eDiscovery Suche erfolgt nun über die Windows PowerShell. Zunächst ist es dabei nötig, sich mit der jeweiligen Cloud zu verbinden.

Zunächst erfolgt dafür die Installation von notwendigen Modulen, präziser das Modul „ExchangeOnlineManagement“ sowie des Package Provider „NuGet“ durch folgende Befehle: [44]

```
Install-Module ExchangeOnlineManagment
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201
Import-Module ExchangeOnlineManagement
```

Sollten bei der Eingabe verschiedene Aufforderungen entstehen, andere Inhalte herunterzuladen, sind diese mit „Ja“ zu bestätigen. Nach der erfolgreichen Installation kann die

Verbindung mit der Cloud hergestellt werden. Dazu werden die folgenden Befehle benötigt: [44]

Connect-ExchangeOnline -Credential $M365credential

In Folge dieses Befehls erscheint ein Fenster, in welchem die Microsoft Anmeldeaufforderung erscheint. In diesem Fenster ist es nun erforderlich, sich mit dem Account eines globalen Administrators anzumelden, um die nachfolgenden Änderungen durchzuführen. [44]

Der letzte Schritt des Verbindungsaufbaus zur Cloud ist das Herstellen einer Verbindung zum Security und Compliance Center herstellen. Dies geschieht über den folgenden Befehl: [44]

Connect-IPPSSession -Credential $M365credential -ConnectionURI https://ps.protection.outlook.com/powershell-liveid/

Sollte die Verbindung erfolgreich gewesen sein, kann man nun neue Compliancegrenzen implementieren. Möglich ist dies durch einen Befehl, der entsprechend konfiguriert werden muss.

New-ComplianceSecurityFilter -FilterName <name of filter> -Users <role groups> -Filters "Mailbox_<MailboxPropertyName> -eq '<Value> '", "SiteContent_Path -like '<SharePointURL>' -or SiteContent_Path -like '<OneDriveURL>'". [44]

Innerhalb dieses Befehls können nun die verschiedenen Variablen definiert werden. [44]

„FilterName“: gibt den Namen der neuen Compliancegrenze an.

„Users“: gibt die Rollengruppe an, für wenn die Compliancegrenze gelten soll.

„Filters“: Gibt im Folgenden die Filter an, welche für die Compliancegrenze gelten soll.

“Mailbox“: Hier werden jegliche Postfächer definiert, welche der „-User“ durchsuchen kann.

„SiteContent“: Hier werden die Seiten definiert, welcher der „-User“ durchsuchen kann.

Um für unser Beispiel nun verschiedene Regeln zu erstellen, wird ebenfalls dieser Befehl verwendet. Voraussetzung ist, dass beispielsweise die E-Mail-Adressen den Namen der jeweiligen Tochtergesellschaften tragen und dass SharePoint Sites einheitlich aufgebaut sind. [44]

Betrachten wir zunächst den Fall für „eDiscovery Manager Frodo“ und die Firma „Auenland“ [44]

> *New-ComplianceSecurityFilter -FilterName "Ring im Auenland" -Users "eDiscovery Manager Frodo”-Filters "Mailbox_Department -eq 'Auenland'", "SiteContent_Path -like 'https://contoso.sharepoint.com/sites/Auenland/*'”*

Mithilfe dieses Filters „Ring im Auenland“ ist es dem eDiscovery Manager „eDiscovery Manager Frodo“ nur noch möglich, Inhalte der Firma „Auenland“ zu durchsuchen, zu betrachten und zu extrahieren. [44]

Für die Firma „Gondor“ und die Rolle „eDiscovery Manager Boromir“ sieht der Befehl ähnlich aus: [44]

> *New-ComplianceSecurityFilter -FilterName "Ring in Gondor" -Users "eDiscovery Manager Boromir”-Filters "Mailbox_Department -eq 'Gondor'", "SiteContent_Path -like 'https://contoso.sharepoint.com/sites/Gondor/*'”*

Die Unterschiede der beiden Befehle beschränken sich zum einen auf die verschiedenen Rollen und die verschiedenen Suchbereiche. Das „*“ am Schluss des SiteContent_Path ist dabei notwendig, damit alle gespeicherten Dateien in diesem Ordner durchsucht werden. Mit der Eingabe dieser Befehle ist die Compliancegrenze eingerichtet und die Begrenzung der Suche mittels Windows PowerShell eingerichtet. [44]

2.3.2 Audit Log

Neben der Möglichkeit zur Einschränkung der Funktionalität von eDiscovery gibt es ebenfalls verschiedene Optionen zur Kontrolle des Werkzeugs eDiscovery innerhalb der M365 Cloud. Eine mögliche Kontrollinstanz ist dabei das Audit Log im Compliance Portal der M365 Cloud. [46]

Das Audit Log ist dabei ein Suchtool, welches die Überwachungsprotokolle in der M365 Cloud durchsucht. In diesen Überwachungsprotokollen werden alle Aktionen gespeichert, welche von Benutzern und Administratoren durchgeführt werden, beispielsweise etwa das Anzeigen eines Dokumentes oder das Löschen einer E-Mail. Nutzbar sind die Funktionen des Audit Logs im Complianceportal. Der Audit Log muss dabei aktiviert sein. Dies ist standardmäßig der Fall. Sollte er deaktiviert sein, ist das Aktivieren über das Complianceportal oder einen PowerShell Befehl möglich. [44]

Um mithilfe des Audit Logs die Überwachungsprotokolle zu durchsuchen, steht unter dem Reiter des Audit Logs im Complianceportal eine Oberfläche zur Verfügung, in welchem man seine Suche eingrenzen kann. Dabei ist es möglich, eine Zeitspanne der Überwachungsprotokolle zu definieren, in welchen gesucht werden soll. Des Weiteren ist es möglich auszuwählen nach welchen Aktivitäten im Überwachungsprotokoll gesucht werden soll. Beispielsweise kann man definieren, welchen Nutzern die Rolle eines „eDiscovery Manager“ zugewiesen wurde, welche Nutzer mithilfe von eDiscovery Dokumente betrachtet haben oder welcher Nutzer über eDiscovery Dokumente extrahiert haben. Die entsprechende grafische Oberfläche ist in Abbildung 6 dargestellt. Das Audit Log ist dabei kein Schutz vor der missbräuchlichen Verwendung von eDiscovery. Es kann aber gezielt nachweisen, welcher Nutzer wann das Werkzeug missbraucht hat und so im Nachhinein die Schuldfrage leichter klären. [44]

Abbildung 6: Erstellung einer Warnungsrichtlinie

2.3.3 Alert Policies

Neben dem Audit Log gibt es eine weitere Kontrollmöglichkeit innerhalb der M365 Cloud, die Alert Policies oder Warnungsrichtlinien. Die Erstellung einer Richtlinie wird in Abbildung 7 gezeigt Diese kann man ebenfalls im Complianceportal konfigurieren. Dabei erstellt man eine Richtlinie, welche man benennt und einen Schweregrad (Niedrig, Mittel, Hoch) sowie eine Kategorie, beispielsweise

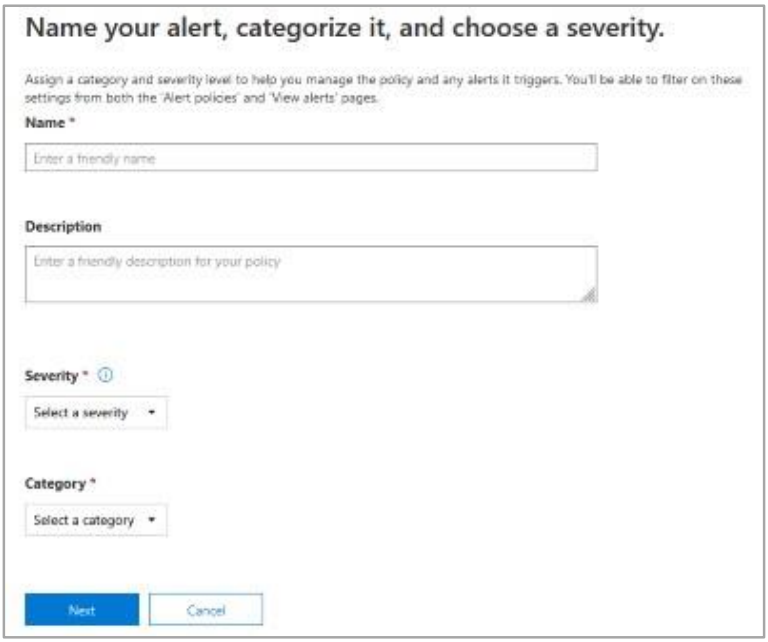


Abbildung 7: Erstellung einer Warnungsrichtlinie

Bedrohungsmanagment, „Informationsgovernance“ oder „Berechtigungen“ für die Richtlinie auswählt. Beispielsweise nennt man die Richtlinie „eDiscovery“, versieht sie mit dem Schweregrad „Hoch“ und der Kategorie „Informationsgovernance.Im weiteren Verlauf des Erstellens der Richtlinie kann man festlegen, bei welcher Bedingung diese ausschlägt. Im Falle einer eDiscovery Richtlinie wäre das möglicherweise das Starten oder Exportieren einer eDiscovery Suche. Im letzten Schritt der Erstellung der Richtlinie wird festgelegt, welche Personen innerhalb der Organisation benachrichtigt werden, sollte die Richtlinie ausgelöst werden. Wenn dies im Ernstfall passiert, so wird jeglichen Mitgliedern, die in dieser Richtlinie festgehalten sind, eine E-Mail geschickt, welche diese benachrichtigt, wer diesen Alarm ausgelöst hat. Im Anschluss können aufgrund dieser Information verschiede Schritte eingeleitet werden, welche optimaler Weise vorher organisationsintern festgelegt wurden. [47]

3 Begrifflichkeiten Datenschutz

Der Begriff Datenschutz und die damit notwendigen Aktionen sind besonders durch die Erstellung der Datenschutzgrundverordnung (DSGVO) ins Bewusstsein der Europäischen Öffentlichkeit gelangt. Im Folgenden Kapitel soll versucht werden, den Begriff des Datenschutzes zu definieren und zu beleuchten, wie dieser in verschiedenen Ländern umgesetzt wird.

3.1 Einordnung des Begriffs Datenschutz

Wenn man den Begriff Datenschutz verwendet, geht es in der allgemeinen öffentlichen Wahrnehmung um den Schutz von Daten. Dies ist aber nicht komplett richtig, der Begriff Datenschutz ist trügerisch. Der Schutz von Daten ist dabei nicht das eigentliche Ziel des Datenschutzes. Dieses liegt vielmehr in dem Schutz der Person. Der Datenschutz soll vor dem Missbrauch oder unangemessener Verarbeitung von personenbezogenen Daten schützen. Dies ist sein primäres Ziel, ein Schutz der Daten wird dadurch indirekt erreicht, ist allerdings wie erwähnt nicht das Hauptziel des Datenschutzes [48p.1]. Eine Verarbeitung von Daten ist dabei jeder Vorgang, automatisiert oder nicht, welcher mit personenbezogenen Daten in Verbindung steht. Dies umfasst beispielsweise das Erfassen, Speichern, Ablesen oder Abfragen sowie die Verwendung dieser Daten. Dies soll im Idealfall nur mit Einwilligung des Betroffenen geschehen [42p.199/33]

Der Hauptgedanke des Datenschutzes ist somit ganz grundlegend das Recht des Einzelnen, individuell darüber zu entscheiden, wie mit seinen persönlichen Daten umgegangen wird und in welchem Umfang sie von verschiedenen Organisationen verwendet werden dürfen. [48p.1]

Der Ursprung der Idee des Datenschutzes basiert dabei auf dem Recht auf informelle Selbstbestimmung und ist eine Form des allgemeinen Persönlichkeitsrechtes und somit der persönlichen Entfaltung. Eine Rechtfertigung zum allgemeinen Überwachen einer Person gibt es nicht, auch wenn diese keine Gründe hätte, etwas zu verbergen. Datenschutz an sich ist kein neues Konzept, so gibt es abgewandelte Formen wie beispielsweise das Beichtgeheimnis oder das Bankgeheimnis schon seit langer Zeit. Durch die Verbreitung der elektronischen Datenverarbeitung steigt allerdings der Bedarf zum Schutz vor einer unangemessenen Nutzung von Daten. [48p.2f]

Innerhalb der Idee des Datenschutzes gibt es dabei verschiedene Grundsätze und Prinzipien, an die sich jegliche spätere Implementierung halten sollte, wenn Datenschutz erfüllt werden soll. Oft bilden diese ein ähnliches Abbild von Prinzipien. Nach ISO/ICE 29100 sind dies beispielsweise: [49p.14]

„Consent and choice“: Die Betroffenen können selbst entscheiden, ob ihre Daten verarbeitet werden oder nicht. [49p.14f]

„Purpose legitimacy and specification“: Die erhobenen personenbezogenen Daten werden lediglich für einen festgelegten, rechtlich erlaubten Zweck verwendet.

„Collection limitation“: Es werden nur die Daten gesammelt, welche für den jeweiligen Zweck notwendig sind und bei denen dies rechtlich erlaubt ist. [49p.15]

„Data minimazation“: Aufbauend auf „collection limitation”. Diese Grundlage besagt, dass auch die weitere Verarbeitung der gesammelten Daten auf ein Minimum beschränkt werden soll. [49p.16]

„Use, rentention and disclosure limitation”: Die Nutzung, Speicherung sowie die Weitergabe der Daten werden auf ein notwendiges Minimum beschränkt. [49p.16]

„Accuracy and quality“: Die verarbeiteten Daten sind richtig, komplett, aktuell und relevant für die weitergehende Nutzung. [49p.16]

„Openness, transparacy and notice“: Es wird transparent und offen mit den Betroffenen kommuniziert, auf welche Art und Weise und für welchen Zweck ihre Daten verarbeitet werden. [49p.17]

„Individual participation and acces“: Die Betroffenen können ihre Daten betrachten und können die überprüfen, korrigieren und ergänzen oder die Löschung ihrer Daten beantragen. [49p.17]

„Acountability“: Innerhalb der Organisation werden verschiedene geeignete, standardisierte Abläufe erstellt, welche dafür sorgen, die Vorgaben des Datenschutzes einzuhalten. Dazu gehören Möglichkeiten zur Dokumentation und Kommunikation. Bei etwaigen Verstößen ist entsprechend diesen Abläufen zu handeln und den Betroffenen zu kontaktieren. [49p.18]

„Information security“: Die Integrität, Verfügbarkeit und Vertraulichkeit der Daten muss gewährleistet sein und gegen externe Angriffe und Einflüsse geschützt sein. [49p.18f]

„Privacy compliance“: Die Einhaltung der verschiedenen Vorgaben bezüglich des Datenschutzes kann nachgewiesen werden und wird durch geeignete Prüfmechanismen kontrolliert. [49p.19]

Will ein Unternehmen Datenschutz einhalten, so müssen diese Grundsätze und Prinzipien bei der Verarbeitung von personenbezogenen Daten in dieser oder ähnlicher Form erfüllt sein. [49p.13]

3.2 Personenbezogene Daten

Wenn wir im Zusammenhang des Datenschutzes über Daten reden, dann sind damit nicht immer alle Daten gemeint. Der Datenschutz soll Missbrauch oder die unangemessene Verarbeitung von personenbezogenen Daten verhindern. Laut Artikel 4 der DSGVO, in welchen personenbezogenen Daten definiert werden, sind diese „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“. [48p.24]

Eine Person wird dabei laut DSGVO als identifizierbar betrachtet, wenn ihnen personenbezogene Daten direkt oder indirekt zugeordnet werden können. Dabei können personenbezogene Daten verschiedenste Formen annehmen. So sind Namen, Kennnummern, Standortdaten oder auch Online-Kennungen wie E-Mail-Adressen Formen von Personenbezogenen Daten. Ebenfalls zu personenbezogenen Daten gehören ein oder mehrere Merkmale, welche Ausdrücke von psychischer, wirtschaftlicher, kultureller, physischer, genetischer, physiologischer oder sozialer Identität dieser Person sind und an welcher sie identifiziert werden kann. [42p.119/33]

Dabei gibt es jedoch auch zwischen den verschiedenen personenbezogenen Daten große Unterschiede, beispielsweise in Hinblick auf ihre Verarbeitung. Innerhalb der EU ist in Artikel 9 der DSGVO geregelt, welche Daten besonders behandelt werden müssen. So ist die Verarbeitung von personenbezogenen Daten untersagt, welche Rückschlüsse auf die „rassische und ethnische Herkunft“, die Gemeinschaftszugehörigkeit, religiöse und oder weltanschauliche Ansichten oder politische Standpunkte zulässt, untersagt. Darüber hinaus ist die Verarbeitung genetischer Daten, Gesundheitsdaten, Daten bezüglich der sexuellen Orientierung und des Sexuallebens allgemein sowie biometrische Daten laut Artikel 9 DSGVO nicht gestattet. [42p.119/33]

Innerhalb des Artikels 9 DSGVO sind allerdings auch Ausnahmen geregelt, welche es erlauben, dass diese spezifischen personenbezogenen Daten verwendet werden dürfen. So ist dies etwa möglich, sollte die Person ausdrücklich eingewilligt haben, dass diese Daten verwendet werden dürfen. Eine andere Möglichkeit wäre, dass die zu verarbeitenden Daten von der Person selbst öffentlich gemacht wurden und so jedem zur Verfügung stehen. Die Verarbeitung dieser personenbezogenen Daten ist ebenfalls zulässig, wenn dadurch lebenswichtige Interessen der Person geschützt werden und die Person selbst außerstande ist, die Einwilligung zur Verarbeitung ihrer Daten zu geben. [42p.119/33]

Neben den personenbezogenen Daten wie Name oder Kennnummern fallen auch Metadaten in das Spektrum der personenbezogenen Daten, solange sie einen Personenbezug haben. Sie unterliegen in diesem Fall dem gleichen Schutz wie „normale“ personenbezogene Daten. Beispielsweise können die Namen von Kommunikationspartnern in Metadaten enthalten sein oder der Zeitpunkt einer Nachricht. Durch diese Daten sind viele Rückschlüsse auf die Person möglich. Besonders innerhalb des Bereiches von IT-Unternehmen sind solche Daten schützenswert, da durch die hohe Verarbeitungsquote mit Daten große Mengen an Metadaten anfallen. [48p.26f]

3.3 Datenschutzregelung in der Europäischen Union

Innerhalb der Europäischen Union gibt es seit 2016 eine einheitliche Regelung für den Datenschutz, die Datenschutzgrundverordnung. Diese Verordnung wurde vom Europäischen Parlament und dem Europarat erarbeitet. Durch verschiedene Gesetze dient diese dem Schutz von natürlichen Personen durch Regelungen und Einschränkungen der Verarbeitung von personenbezogenen Daten. Dieser Schutz vor unrechtmäßiger Verarbeitung personenbezogener Daten wurde durch diese Verordnung gleichzeitig zu einem Grundrecht für alle Menschen erklärt [48p.19]. Als Verordnung der Europäischen Union gilt die Datenschutzgrundverordnung für alle Staaten der Europäischen Union. Die DSGVO enthält somit bereits gültiges und anwendbares Recht allein durch ihren Status als EU-Verordnung. Sollte die Rechtslage nicht klar sein, so hat die DSGVO im Zweifelsfall auch Vorrang vor nationalen Recht der Mitgliedsstaaten der Europäischen Union. So ist eine grundlegende Regelung, welche durch die DSGVO Rechtmäßigkeit erlangt, dass personenbezogene Daten nicht verarbeitet werden dürfen, es sei denn, dies ist ausdrücklich von dem Träger der personenbezogenen Daten gestattet. [48p6]

In der DSGVO sind in Artikel 5 dabei verschiedene Grundsätze geregelt, welche für die Verarbeitung von personenbezogenen Daten gelten. Diese sind im Folgenden: [42p.119/35]

„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“:
In diesem Grundsatz wird ausgesagt, dass Verarbeitung von personenbezogenen Daten ohne ausdrückliche Einwilligung nicht gestattet ist (Rechtmäßigkeit). Des Weiteren soll hiermit verhindert werden, dass ein Verantwortlicher, welcher Zugriff auf personenbezogene Daten hat, diesen ausnutzt, auch wenn diese nicht konkret gegen ein Gesetz verstößt (Verarbeitung nach Treu und Glaube). Jegliche Verarbeitung von personenbezogenen Daten muss dabei für die Betroffenen sichtlich gemacht werden und nachvollziehbar sein. Eine heimliche Erfassung und Verarbeitung von Daten ist somit nicht erlaubt (Transparenz). [42p.119/35]

„Zweckbindung“
Die erhobenen personenbezogenen Daten dürfen lediglich für den Zweck verwendet werden, für welchen sie ursprünglich erhoben wurden und für keine andere Funktion. In Artikel 6 DSGVO sind dabei die verschiedenen Kriterien definiert, welche hierbei erfüllt werden müssen. [42p.119/35]

„Datenminimierung“
Es sollen nur die Daten erfasst werden, welche auch für die jeweilige Verarbeitung erforderlich sind. Eine Speicherung von für den Fall unerheblichen Daten ist nicht gestattet. [42p.119/35]

„Richtigkeit“
Die erhobenen Daten müssen auf dem neuesten Stand sein. Es gilt im Umkehrschluss angemessene Maßnahmen zu treffen, um mögliche falsche, nicht aktuelle Daten zu identifizieren und in Folge zu löschen oder zu berichtigen. [42p.119/35]

„Speicherbegrenzung“
Die Speicherung der personenbezogenen Daten darf nicht länger geschehen, als es für den jeweiligen Zweck erforderlich ist. [42p.119/35]

„Integrität und Vertraulichkeit“
Die Verarbeitung der personenbezogenen Daten muss so erfolgen, dass eine angemessene Sicherheit der Daten gewährleistet wird. So ist es essenziell, dass ein Schutz vor nicht befugter oder unrechtmäßiger Verarbeitung, nicht beabsichtigtem Verlust oder Beschädigung implementiert wird. Dabei sind verschiedene organisatorische und technische Maßnahmen zu ergreifen. [42p.119/35]

„Rechenschaftsplicht“
Für die Einhaltung der verschiedenen Grundsätze gibt es einen Verantwortlichen, welcher die Einhaltung der einzelnen Punkte nachweisen können muss. [42p.119/35]

Neben diesen Grundsätzen sind auch verschiedene Bedingungen definiert, in welchen die Verarbeitung von personenbezogenen Daten möglich ist, ohne dass diese einen strafbaren Datenschutzverstoß darstellen. So regelt beispielsweise Artikel 2 DSGVO bestimmte Ausnahmen, sollte die Verarbeitung von Daten durch Behörden geschehen. Des Weiteren werden in Artikel 6 DSGVO noch weitere Ausnahmen definiert, in welchem die Verarbeitung personenbezogener Daten erlaubt ist, beispielsweise wenn sie zu Erfüllung einer rechtlichen Pflicht benötigt wird. [42p.119/35]

3.3.1 Datenschutzregelung in Deutschland

Als Mitgliedsland der Europäischen Union gilt die Datenschutzgrundverordnung und die damit verbundenen Regellungen in Deutschland. Eine Notwendigkeit für ein eigenständiges nationales Recht besteht somit nicht, da durch die DSGVO bereits Regelungen, Vorschriften sowie Gesetzte definiert sind, diese angewendet werden können und nationales Recht hinter dieser Verordnung zurücksteht. Innerhalb Deutschlands gibt es nichtsdestotrotz das Bundesdatenschutzgesetzt (BDSG). Dieses Gesetz stellt dabei allerdings kein autarkes Regelwerk dar, sondern bietet vielmehr verschiedene Ergänzungen zur DSGVO. Somit ist es durch das BDSG lediglich möglich, die verschiedenen Gesetze zu konkretisieren, nicht jedoch diese zu ändern. [48p.7]

Das zeigt sich auch in dem Leitfaden, der von dem Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BFDI) gestellt wurde. In diesem ist ebenfalls von verschiedenen Grundsätzen die Rede, welche eingehalten werden müssen, um Datenschutz in Organisationen zu gewährleisten. Diese orientieren sich dabei stark an Artikel 5 der DSGVO. Das Standard-Datenschutzmodell enthält folgende Grundsätze (welche denen der DSGVO stark ähneln): [50]

Datenminimierung:
Bei der Verarbeitung von personenbezogenen Daten ist diese auf ein notwendiges, dem Zweck angemessenes Maß zu beschränken.[50]

Verfügbarkeit:
Die Möglichkeit, auf personenbezogene Daten unverzüglich zuzugreifen, muss gegeben sein, gleichzeitig muss ihre Verarbeitung ebenfalls unverzüglich geschehen. Darüber hinaus muss gesichert sein, dass die Verarbeitung der Daten im vorgesehenen Prozess ordnungsgemäß vonstattengeht. [50]

Integrität:
Personenbezogene Daten dürfen nur auf so eine Art und Weise verarbeitet werden, welche einen Schutz vor (unbeabsichtigtem) Verlust, (unbeabsichtigter), Zerstörung oder Schädigung durch organisatorische oder technische Maßnahmen gewährleistet. Die Gesamtheit der Veränderungen an den gespeicherten Daten durch beispielsweise unautorisierte Dritte, soll im Idealfall ausgeschlossen werden oder aber kenntlich gemacht werden und dadurch reversibel sein. [50]

Vertraulichkeit:
Es dürfen lediglich befugte Personen Daten zur Kenntnis nehmen oder diese nutzen. Unbefugten Personen ist dies nicht gestattet. [50]

Nichtverkettung:
Wenn personenbezogenen Daten für unterschiedliche Zwecke erhoben wurden, dann dürfen diese nicht zusammengeführt werden, daher verkettet werden. [50]

Transparenz:
Es muss klar erkennbar sein, zu welchem Zweck welche Daten erhoben und verarbeitet werden. Darüber hinaus muss gezeigt werden, welche Systeme und Prozesse genutzt werden, um sie zu verarbeiten und um zu zeigen, wohin die Daten zu welchem Zweck fließen. Ebenfalls muss gezeigt werden, wer die rechtliche Verantwortung für die personenbezogenen Daten und Systeme in den unterschiedlichen Phasen einer Datenverarbeitung trägt.[50]

Intervenierbarkeit:
Alle Betroffenen der personenbezogenen Daten müssen ihre Rechte an diesen wahrnehmen können, d.h. sie können Auskunft über ihre Daten erlangen, Korrekturen durchführen lassen oder ihre personenbezogenen Daten löschen oder sperren. Im Umkehrschluss bedeutet dies, dass alle Verarbeitungsprozesse so gestaltet sind, dass dies erfolgen kann.[50]

3.3.2 Datenschutzregelung in Österreich

Ähnlich zu der Situation in Deutschland besitzt Österreich an sich wenig Möglichkeit, die Datenschutzregelungen zu modifizieren, da sie ebenso Teil der Europäischen Union sind und so die DSGVO gilt. Trotz dessen gibt es ein Gesetz, welches dazu dient, die DSGVO zu konkretisieren und zu erweitern. In Österreich ist dies, dass Datenschutzgesetz (DSG) welche oben erwähnte Aufgaben übernimmt. Besonders erwähnenswert ist hier, dass vor der DSGVO es bereits ähnliche Regelungen in einem nationalen Gesetz Österreichs gab, wodurch Datenschutz rechtlich verankert war. Diese verschiedenen Regelungen wurden mit Einführung der DSGVO in diese internationale Verordnung verschoben. Weitere Änderungen an den Datenschutz in Österreich brachte die DSGVO nicht. [48p.8]

Innerhalb von Österreich gelten damit die verschiedenen Prinzipien der DSGVO, genauer beschrieben in Kapitel 3.3: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht. Diese verschiedenen Prinzipien müssen erfüllt werden, sollte der Datenschutz in vollem Umfang gewährleistet werden. [48p.8]

3.4 Datenschutzregelung in den USA

Aufgrund dessen, dass viele Cloud Anbieter, etwa Microsoft, ihren Stammsitz in den Vereinigten Staaten von Amerika haben, ist der dortige Stand des Datenschutzes von erheblichem Interesse für europäische Unternehmen und ihre Entscheidungen.

3.4.1 Gesetzliche Datenschutzregelung

Besonders bedeutend für Entscheidungen von Organisationen ist der Stand des Datenschutzes innerhalb des Landes, dessen Dienste beispielsweise Cloud-Dienste sie beanspruchen. So auch im Fall mit den Vereinigten Staaten von Amerika. Hierbei gibt es allerdings eine Besonderheit, anders als innerhalb der Europäischen Union gibt es innerhalb der Vereinigten Staaten kein einheitliches Recht bezüglich des Datenschutzes. Es ist momentan viel eher so, dass verschiedene Branchen unterschiedliche Datenschutzvorschriften besitzen. So haben etwa die Sektoren der Erziehung und der Krankenversicherung unterschiedliche Vorschriften und Richtlinien bezüglich der datenschutzregelungen. Darüber hinaus gibt es ebenfalls von Bundesstaat zu Bundesstaat verschiedene Regelungen des Datenschutzes, welche allerdings nur für dieses Bundesland gelten. Es gibt kein einziges Gesetz in den USA, welches alle personenbezogenen Daten abdeckt und Datenschutz gewährleistet. Somit sind die Vereinigten Staaten von Amerika Datenschutzrechtlich betrachtet ein einziger Flickenteppich an Regelungen, wie in Abbildung 8 dargestellt. [51]

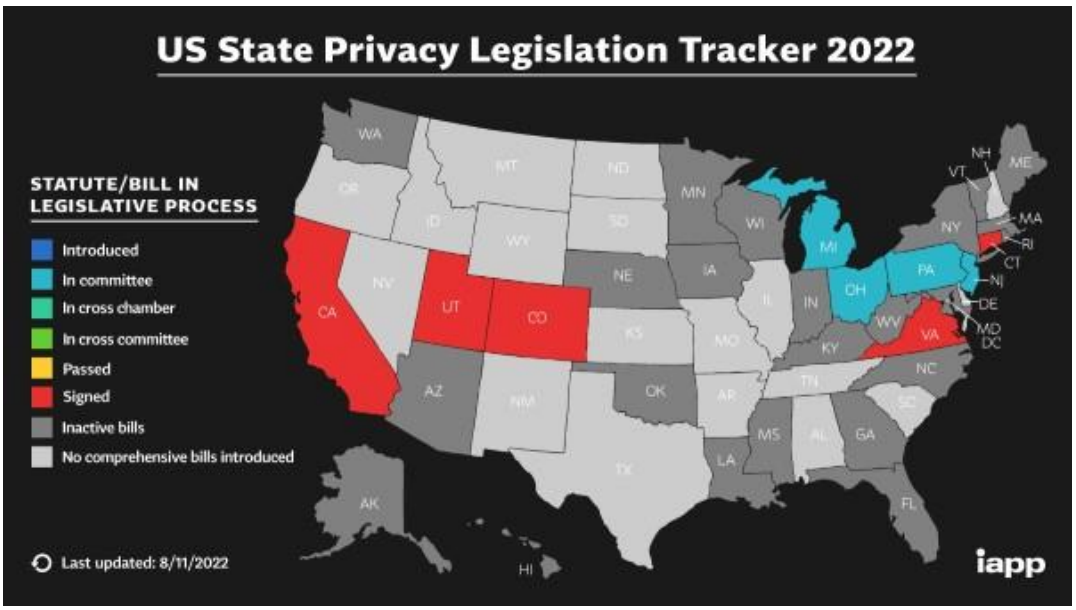


Abbildung 8: Stand der Datenschutzregelungen in den USA, entnommen aus [52]

Es bestehen dabei verschiedene Unterschiede zwischen den Regelungen in der Europäischen Union und den Vereinigten Staaten von Amerika. Prinzipiell wird in den USA das Recht auf freie Meinungsäußerung höher gehalten als das Recht des Datenschutzes. Dies

kann zu gewissen Konflikten führen, etwa wenn in Folge der Meinungsäußerungen personenbezogene Daten, wie etwa Namen und Bilder veröffentlicht werden. [48p.11]

Eine andere wichtige Rolle bei der Umsetzung des Datenschutzes in den USA ist die „Federal Trade Comission“. Diese Kommission sorgt dafür, dass die Zusagen, welche Organisationen an ihre Kunden geben, auch tatsächlich eingehalten werden. So auch wenn eine Organisation Datenschutz verspricht. Sollte dies der Fall sein, dann prüft die „Federal Trade Comission“ ob dies auch wirklich eingehalten wird. Gibt es Abweichungen von den Versprechen der Organisation geben, werden diese mit Sanktionen bestraft. [48p.11]

Ein weiterer bedeutsamer Unterschied zwischen den Datenschutzregelungen der beiden Regionen ist das Vorhandensein von Aufsichtsbehörden des Staates und Datenschutzbeauftragten innerhalb der Unternehmen. So sind diese in der Europäischen Union im Datenschutz stark verankert. Diese bieten Kontrollinstanzen, welche für die Sicherheit der personenbezogenen Daten von Bedeutung sind. Innerhalb der Vereinigten Staaten von Amerika gibt es solche Instanzen weniger. Als logische Folge sind Kontrollen hinsichtlich des Datenschutzes innerhalb der Vereinigten Staaten seltener als in der Europäischen Union. [48p.11]

In den Vereinigten Staaten von Amerika ist es möglich, dass personenbezogenen Daten verwendet, geteilt oder gar verkauft werden, wenn die datenhaltende Organisation dies möchte. Dabei werden die davon Betroffenen nicht informiert, selbst bei einem Verkauf ihrer eigenen Daten. Es ist selbst möglich, dass eine Organisation die Daten mit einer anderen teilt, welche diese dann verkauft, ohne dass der Betroffene auch nur eine Information dahingehend bekommt. Es ist für die Betroffenen nicht nachvollziehbar, welche Organisation am Ende im Besitz ihrer personenbezogenen Daten ist. [48p.11]

Die verschiedenen Datenschutzprinzipien, welche in der Europäischen Union gelten, haben in den Vereinigten Staaten von Amerika keine Bedeutung. So sind beispielsweise Grundsätze wie Datenminimierung oder die Zustimmung zur Verarbeitung von Daten nicht vorhanden.

3.4.2 Gesetzliche Möglichkeiten zum Zugriff auf Daten

Im Gegensatz zu den nicht vorhanden gesetzlichen Regelungen vonseiten der Regierung hinsichtlich Datenschutzes gibt es sehr wohl verschiedene Gesetze und Verordnungen, welche es der Regierung ermöglichen, auf Daten von in den USA ansässigen Unternehmen und Organisationen zuzugreifen. Dazu gehören auch oder gar ganz besonders personenbezogene Daten. Durch diese Regelungen sind somit US-amerikanische Behörden wie das

FBI oder die NSA legal dazu ermächtigt, auf diese Daten zuzugreifen und diese zu verwenden. [48p.11]

3.4.2.1 FISA

Die Grundlage dieser Regelungen und die Positionierung und entsprechende Handlung der US-amerikanischen Regierung gehen dabei weit zurück bis in die Zeiten des Kalten Kriegs. Erste Grundlagen wurden bereits 1978 mit dem Foreign Intelligence Surveillance Act (FISA) gelegt [53]. Mithilfe dieses Gesetzes ist es den Nachrichtendiensten möglich, Telekommunikation von nicht US-Bürgern im Ausland zu überwachen, ohne dass dies individuell genehmigt werden muss [54]. Eine formelle Genehmigung erfolgt durch ein durch dieses Gesetz geschaffene Gericht, welches nicht öffentlich tagt. Als Grundlage dafür besteht der Verdacht, dass nachfolgende Überwachung für den Zweck der Terrorismusabwehr relevant sind. Diese Überwachung beschränkt sich dabei nicht nur auf die Kommunikation, welche von der Zielperson ausgeht, und empfängt. Es können ebenfalls unbeteiligte Dritte abgehört werden, sollte diese aufgrund welchen Grundes auch immer Informationen über die Zielperson besitzen und diese verbreiten. Eine Einschränkung hinsichtlich der Art der Daten, welche durch diese Überwachung erlangt werden, gibt es nicht. [55]

3.4.2.2 Patriot Act

Erweitert wurde dieses Gesetz dabei nach den Terroranschlägen des 11. Septembers 2001. In Folge dieses traumatischen Ereignisses für die Vereinigten Staaten wurden der USA Patriot Act (Uniting and Strengtheninng America by Providing Appropriate Tools Required ot Intercept and Obstruct Terrorism Act) von US-amerikanischen Kongress verabschiedet, um gegen weitere mögliche Terroranschläge präventiv handeln zu können [56]. Dieser bietet für die Nachrichtendienste der Vereinigten Staaten, verschiedene Handlungsmöglichkeiten, wie etwa das Einsehen von Bankdaten durch das FBI, ohne das Beweise für ein Verbrechen vorliegen. Eine andere für die Geheimdienste nun legale Option ist es, auf Server von US-Unternehmen zuzugreifen, ohne dass dies einen richterlichen Bescheid benötigt. Betroffen sind davon aber nicht nur US-Unternehmen. Diese Regelung, welche Zugriff auf die verschiedenen Server gewährt, gilt auch für Tochterfirmen von US-Unternehmen, diese müssen im Zuge dieses Gesetzes ebenfalls Zugriff auf ihre Server gewähren. Bei Letzterem ist es dabei nicht von Bedeutung, ob nationale Gesetze andere Regelungen vorsehen. Die Speicherung der so erlangten Daten erfolgt intern bei der NSA und enthalten neben beispielsweise E-Mails auch Telefongespräche [55]. In Folge der Bekanntmachung durch Edward Snowden wurde verbreitet, dass beispielsweise Microsoft Dienste wie Skype oder Outlook ständig der NSA zugänglich waren. [57]

3.4.2.3 Freedom Act

Im Jahr 2015 wurde der „USA Patriot Act“ nach zuvor doppelter Verlängerung nicht verlängert. Einige der Regelungen, welche innerhalb des „USA Patriot Act“ vorhanden waren, wurden in einem neuen Gesetz, mit leichten Veränderungen, fortgeführt. Dieses neue Gesetz ist der USA Freedom Act (Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act). Ein großer Unterschied dieses Gesetzes im Vergleich mit dem „USA Patriot Act“ ist die Speicherung von Daten. Während es durch den Patriot Act möglich war, dass Geheimdienste die verschiedenen Telekommunikationsdaten selbst speichern und so direkten Zugriff auf ebenjene haben, ist dies durch das neue Gesetz nicht mehr der Fall. Dies untersagt die Speicherung dieser Daten für Geheimdienstbehörden und unterbindet so den direkten Zugriff. Die Speicherung der Daten erfolgt allerdings noch immer durch die verschiedenen Kommunikationsunternehmen. Auf das Verlangen der Geheimdienste müssen diese Unternehmen ihre Daten an die verschiedenen Nachrichtendienste weiterleiten. Als einzige Voraussetzung ist hierbei gegeben, dass die Betroffenen Personen laut Geheimdiensten eine potenzielle Gefahr darstellen. Sollte diese Voraussetzung erfüllt sein, steht einer ausführlichen Datenüberwachung und Analyse durch die Geheimdienste nichts im Wege.[58]

3.4.2.4 Cloud Act

Ein weiteres Gesetz, welches Zugriff von US-amerikanischen Behörden auf personenbezogenen Daten erlaubt, ist der Cloud Act. Cloud steht dabei für “Clarifying Lawful Overseas Use of Data Act” und nicht für das Konzept Cloud an sich.

Dieses Gesetz verpflichtet alle IT-Dienstleister, welche in den Vereinigten Staaten ansässig sind, die ihnen zur Verfügung stehenden Daten an die Behörden weiterzuleiten, selbst wenn diese nicht in den Vereinigten Staaten gespeichert sind. Im Gegenzug soll es ebenfalls ausländischen Behörden ermöglicht werden, auf Daten zuzugreifen, welche auf amerikanischen Servern liegen. [59]

Aufgrund dieses Gesetzes sollen Abkommen zwischen den Ländern getroffen werden, welche den Zugriff auf Daten, darunter auch personenbezogenen Daten regelt. Im Allgemeinen soll es den jeweiligen Behörden möglich sein, sich direkt an die Unternehmen zu wenden, welche die Daten besitzen und diese anzufragen. Eine richterliche Erlaubnis wird nach diesem Prinzip nicht mehr benötigt, um auf Daten zuzugreifen. [59]

4 Technische Einschränkungen von eDiscovery in der M365 Cloud zum Gewährleisten des Datenschutzes

4.1 Mögliche Einschränkungen in der Europäischen Union

Als extrem mächtiges Suchwerkzeug steht eDiscovery, unter der Voraussetzung einer passenden Lizenz jedem Unternehmen zur Anwendung bereit. Aufgrund seiner Natur als Suchwerkzeug jede einzelne Datei zu durchsuchen, welche innerhalb der Cloud gespeichert ist, sind verschiedene Einschränkungen notwendig. Diese Einschränkungen haben dabei verschiedene Gründe, zum einen ist es problematisch, wenn ein Angehöriger der Rolle eDiscovery Manager (oder einer Rolle mit ähnlichen Rechten) alle Dokumente einer Organisation durchsuchen und betrachten kann, ohne dafür eigentlich berechtigt zu sein. Ein anderer Grund sind die möglicherweise resultierenden Datenschutzverstöße, welche durch einen so unregulierten Einsatz von eDiscovery entstehen könnten. Diese Verstöße hätten hohe finanzielle Entschädigungen zur Folge. Um diesen Konsequenzen entgegenzuwirken, ist es nötig, verschiedene Kontrollmechanismen einzuführen.

Da die Ansprüche an den Datenschutz sowohl in Deutschland als auch in Österreich aufgrund der Datenschutzgrundverordnung beinahe identisch sind, werden im Folgenden beide gemeinsam in diesem Kapitel als „Europäische Union“ betrachtet. Da die Datenschutzgrundverordnung, wenn auch teilweise mit anderen Namen, im gesamten Gebiet der Europäischen Union gilt, sind auch in anderen dazugehörigen Ländern die Anforderungen an den Datenschutz ähnlich.

Die Kernpunkte, welche nun für den Datenschutz betrachtet werden müssen, sind je nach Model leicht verschieden. Da die Länder nun innerhalb der Europäischen Union liegen, sind die Grundsätze der Datenschutzgrundverordnung zum Prüfen naheliegend. Diese sind, wie bereits ausgeführt: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht

Sollten alle dieser Voraussetzungen erfüllt werden, so steht einer entsprechenden Verwendung von eDiscovery nichts mehr im Weg. Die einzelnen Möglichkeiten zur Verwendung von eDiscovery sind, wie bereits erwähnt, juristische Prozesse. Hier ist dabei zu unterscheiden, ob diese Verwendung dabei durch das Gericht legitimiert ist oder ob eine Organisation dies selbstständig tut, um Beweise vorzulegen. Eine andere Möglichkeit,

welche im Folgenden betrachtet wird, ist die nicht juristische Art, so etwa Ermittlungen beim Veröffentlichen von sensiblen Dokumenten oder bei Mobbingerfahrungen. Die letzte Betrachtung umfasst Datenschutzanfragen gemäß Artikel 15 DSGVO, bei welchen eDiscovery als Mittel verwendet werden kann.

Dabei ist hervorzuheben, dass es bei der Betrachtung vor Gericht nicht um das Werkzeug oder den Prozess eDiscovery als solches geht. Es ist vielmehr wichtig, welche Erkenntnisse durch den Prozess oder dem Werkzeug in der M365 Cloud gewonnen werden können. Sowohl der Prozess als auch das Werkzeug stellen dabei Verstöße gegen die Idee des Datenschutzes dar.

Als Grundlage sei bereits hier angemerkt, dass in jeglichem aufgeführten Fall in der Regel die Kontrollinstanzen von Audit Log und Alert Policies aktiviert sein sollen. So kann zwar durch diese keine Einschränkung des Werkzeugs eDiscovery erfolgen, wohl aber ist so zumindest eine Vorwarnung gegeben und etwaige entstehende Datenschutzverstöße können im Nachhinein leichter aufgedeckt werden.

4.1.1 Juristischer Prozess mit Gerichtseinfluss (EU)

Betrachten wir nun als erste Variante die Nutzung von eDiscovery, sollte es im Rahmen eines juristischen Prozesses verwendet werden. Die Grundsätze, welche durch dieses Prozedere verletzt werden, wären vor allem die der Zweckbindung (aufgrund der Verwendung abseits des von dem Betroffenen genehmigten Zweckes), Transparenz (sollte nicht umgehend eine Mitteilung der Betroffenen erfolgen) sowie der Rechtmäßigkeit (die Betroffenen haben nicht eingewilligt, dass ihre personenbezogenen Daten auf diese Art verwendet werden). Die anderen Prinzipien, welche die Datenschutzgrundverordnung vorgibt, um ebenjenem Datenschutz zu gewährleisten, werden dabei nicht oder nicht in diesem Maße verletzt.

Sollte nun im Falle dieser juristischen Untersuchung vom Gericht ein Untersuchungsbeschluss erlassen werden, welche es den Behörden erlaubt, direkt oder indirekt eDiscovery zu verwenden, so sind auch die Verstöße gegen die Prinzipien der Datenschutzgrundverordnung zulässig. Dies ist geregelt in Artikel 2 der Datenschutzgrundverordnung. Dort wird festgehalten, dass die Datenschutzgrundverordnung nicht angewendet wird, sollten personenbezogene Daten „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ verarbeitet werden. Insofern sind die Verstöße gegen die Prinzipien des Datenschutzes in diesem Fall legitimiert, wenn diese durch die Behörden geschehen und für eine Straftat relevant sind.

Wenn die Behörden sich nun entscheiden, im Zuge ihrer Aufklärung das Werkzeug eDiscovery in der M365 Cloud zu verwenden, sind keine technischen Einschränkungen nötig, um Datenschutz zu gewährleisten, eben weil Verstöße gegen die Grundsätze der Verarbeitung von personenbezogenen Daten gestattet sind. Ob trotz dessen verschiedene Einschränkungen für die Nutzung von eDiscovery angewandt werden, etwa um die Suchzeit zu verkürzen oder die Suche leichter zu spezifizieren, bleibt offen. Andere Kontrollinstanzen wie etwa eine Dokumentation der eDiscovery Suche bleiben unumgänglich, schon aus dem Grunde, da sich damit sowohl Behörde als auch Organisation absichern können, falls personenbezogene Daten veröffentlicht werden. Um diesen Verstoß im Nachgang zu rekonstruieren, ist eine Dokumentation essenziell.

4.1.2 Juristischer Prozess ohne Gerichtseinfluss (EU)

Im anderen Fall des juristischen Verfahrens gibt es kein Durchsuchungsbeschluss vonseiten des Gerichtes für die Behörden. Vielmehr ist das Szenario die Nutzung des Werkzeugs eDiscovery vonseiten eines Unternehmens. Mithilfe des Suchtools sollen dabei beispielsweise Indizien gefunden werden und die eigene Argumentation untermauert werden.

Hierzu gibt es nun zwei verschiedene Möglichkeiten, wie eDiscovery verwendet wird. Ausschlaggebend dafür ist, welche Einwilligung vonseiten der Betroffenen in Bezug auf die Verarbeitung ihre personenbezogenen Daten gegeben wurden.

Sollten die Betroffenen ihre Einwilligung geben und so eingewilligt haben, dass ihre personenbezogenen Daten während der Speicherung auch für potenzielle Gerichtsprozesse durchsucht und verwendet werden können, so ist eDiscovery ohne Bedenken nutzbar.Technische Einschränkungen sind hier nicht nötig, um den Datenschutz umzusetzen, wohl aber vonseiten der Organisation wünschenswert, um etwa streng vertrauliche Dokumente nicht zu durchsuchen und generell die betreffende Suche und Dokumentenmenge so klein wie möglich zu halten, um den Prozess zu beschleunigen. Es wäre hier beispielsweise eine Einschränkung der SharePoint-Sites zu empfehlen.

Die andere Variante ist, dass es keine solche Einwilligung der Betroffenen gab. Die personenbezogenen Daten können damit nicht für dieses gerichtliche Verfahren verwendet werden. Die Möglichkeiten der Nutzung von eDiscovery sind hier stark beschränkt, da es möglich und wahrscheinlich ist, dass personenbezogenen Daten in den Dokumenten oder E-Mails enthalten sind, so stellt bereits eine E-Mail-Adresse ein personenbezogenes Datum dar und damit einen Datenschutzverstoß dar.

Eine Lösung dieses Problems stellt sich als kompliziert heraus und ist je nach Ausgangssituation der Organisationen unterschiedlich.

Eine erste Lösungsoption wäre, per E-Mail eine Aktualisierung der Verarbeitung von personenbezogenen Daten an alle Betroffenen zu schicken, welche eben jene Verarbeitung

für einen Prozess inkludiert und um eine Einwilligungsbestätigung zu bitten. Im Folgenden wäre es möglich, die Dateien der Betroffenen, welche diese Einwilligungen akzeptieren, in einen neuen Ordner zu kopieren und einen Filter einzurichten, welcher es erlaubt, nur in diesem Ordner eDiscovery zu verwenden. Ein ähnliches Vorgehen wäre bei jeglichem E-Mail Verkehr notwendig. So müssen die E-Mails der Betroffenen, welche ihre Einwilligung gegeben haben, kopiert werden und ebenfalls in den Filter eingepflegt werden. Ob diese Variante am Ende eine Kosten-Nutzen-Analyse übersteht, ist jedoch fraglich. Es ist möglich, dass in diesem Szenario auf eine Verwendung des Werkzeugs eDiscovery verzichtet wird, da der notwendige Aufwand, um es datenschutzkonform durchzuführen, zu groß ist.

Eine andere Variante, um eDiscovery in einem Gerichtsverfahren zu benutzen, ist, wenn das Verarbeiten von personenbezogenen Daten zur Wahrung und zum Schutz der berechtigten Interessen der Organisation dient und nicht die Grundrechte und Freiheiten der Betroffenen überwiegen. Sollte diese Abwägung zugunsten der Organisation ausfallen, so steht es dieser offen, eDiscovery zu verwenden. Einschränkungen hier wären nicht notwendig, um den Datenschutz zu gewährleisten, wohl aber um die Suche effizienter zu gestalten.

4.1.3 Interne Untersuchung: Katastrophenfall (EU)

Weitere Situationen, in welchen eDiscovery verwendet werden kann, ist in Szenarien einer internen Untersuchung in der Organisation, beispielsweise im Katastrophenfall, bei der Veröffentlichung von streng vertraulichen Dokumenten oder bei dem Verdacht von Geldwäsche gegeben. In diesen Fällen darf eDiscovery verwendet werden, um alle Daten zu durchsuchen. Grund hierfür ist ebenfalls Artikel 6 der Datenschutzgrundverordnung.

Wie bereits erwähnt, ist die Verarbeitung von personenbezogenen Daten erlaubt, wenn die Interessen der verarbeitenden Organisation als größer einzuschätzen sind als die Interessen der Betroffenen. Im Katastrophenfall einer Organisation ist es wahrscheinlich, dass dieser Umstand eintritt. Einschränkungen des eDiscovery Werkzeuges sind hier nicht nötig, um Datenschutz zu gewährleisten. Wohl aber sind Einschränkungen wahrscheinlich, um die Suche zu optimieren und zu beschleunigen.

4.1.4 Interne Untersuchung: Mitarbeiterkritik (EU)

Ein weiteres Szenario, in welchem eDiscovery eingesetzt werden kann, ist das der Mitarbeiterkritik. Dabei müssen hier verschiedene Varianten unterschieden werden. Zum einen, wenn sich ein Mitarbeiter der Organisation bei der dazugehörigen Stelle über Mobbing oder Diskriminierungserfahrung ausspricht und diese anzeigt. Die andere Variante ist, dass es keine Beschwerden vonseiten der Mitarbeiter gibt. Hier will im Gegensatz aber das

Unternehmen herausfinden, was Mitarbeiter über das Unternehmen innerhalb der Cloud sagen und wie zufrieden sie sind.

Betrachten wir zunächst die erste Variante, hier ist es fraglich, ob die Begründung des größeren Interesses der Organisation gegenüber den Freiheiten des Einzelnen angewendet werden kann. Wenn wir nun davon ausgehen, dass dieser Grundsatz angewendet wird, so ist die Nutzung von eDiscovery möglich. Technische Einschränkungen wären hier notwendig, so etwa, um genau die Dokumente der in Verdacht stehenden Abteilungen zu durchsuchen. Das gesamte Unternehmen zu durchsuchen wäre unverhältnismäßig. Der Vorteil bei der Verwendung von eDiscovery, ist dabei die Möglichkeit, dass nachgewiesen werden kann, welche Dokumente betrachtet werden. Ebenso können diese nicht nachträglich verändert werden, da eine Kopie von ihnen angefertigt wurde, wenn sie mithilfe von eDiscovery gefunden wurden. Wenn diese Annahmen nicht gelten, so ist das Werkzeug eDiscovery nicht verwendbar, egal welche technischen Einschränkungen auch gegeben sind, da zwangsläufig auch personenbezogene Daten von nicht Betroffenen verarbeitet wird, selbst wenn man nur das Konto der beschuldigten Person durchsucht. Es muss eine andere Möglichkeit gefunden werden, um diese Beschuldigungen nachzuweisen. Hilfreich wären hier interne Prozesse, welche zur Klärung solcher Beschwerden eingerichtet wurden.

In der anderen Variante des Szenarios ist die Nutzung von eDiscovery nicht möglich. Das Interesse der Organisation steht hier eindeutig nicht über den Freiheiten der Betroffenen, in diesem Fall den Mitarbeitenden der Organisation. Die Meinungsfreiheit dieser Personen ist in jedem Fall höher zu werten als der Wille der Organisation, Kritik aufzuspüren. Infolgedessen ist eDiscovery nicht verwendbar, egal welche Einschränkungen auch getroffen werden.

4.1.5 Datenschutzanfragen

Eine weitere Möglichkeit, wie eDiscovery im täglichen Arbeiten einer Organisation angewandt werden kann, ist die Verarbeitung von Datenschutzanfragen. Mit dem Inkrafttreten der Datenschutzgrundverordnung hat jede Person das Recht zu erfahren, in welcher Art und Weise ihre Daten von Unternehmen verwendet werden, welche in der Europäischen Union arbeiten. Aus diesem Anspruch heraus bilden sich ebenjene Datenschutzanfragen [42 p.119/43]. Diese müssen innerhalb eines Zeitraums von 30 Tagen nach Eingang beantwortet werden [42 p.119/40]. Enthalten sind in dieser Antwort alle Dokumente des Unternehmens in welchen die personenbezogenen Daten des Anfragenden verwendet werden. [42 p.119/43]

Als Suchwerkzeug bietet eDiscovery genau die Funktionen, die benötigt werden, um ebenjene Dokumente zu finden und zu exportieren. Technische Einschränkungen, um den Datenschutz umzusetzen, sind in diesem Szenario nicht erforderlich. Die Verarbeitung von personenbezogenen Daten ist gestattet, um rechtliche Verpflichtungen zu erfüllen, laut Artikel 6 DSGVO. Eine Datenschutzanfrage ist genauso eine Verpflichtung, welche jede

Organisation nachkommen muss. Weitere technischen Einschränkungen wären nicht erforderlich, da der Anspruch einer Datenschutzanfrage ein möglichst vollständiger Korpus an Dokumenten ist. Jegliche Art von Einschränkungen würde diesem Anspruch widersprechen.

Zu beachten dabei ist, dass bei der Übergabe an den Anfragen in der Regel alle Angaben geschwärzt werden, welche nicht seine personenbezogenen Daten umfassen. Dies geht von internen Dokumenten bis hin zu personenbezogenen Daten Dritter.

4.2 Mögliche Einschränkungen in den Vereinigten Staaten von Amerika

Die Betrachtung von Datenschutz innerhalb den Vereinigten Staaten von Amerika gestaltet sich schwieriger als die Betrachtung des Datenschutzes in der Europäischen Union und ihren angehörigen Staaten. Der Grund dafür liegt in dem nicht Vorhandensein einer einheitlichen, alle US-amerikanischen Bundesstaaten umfassenden Datenschutz-regelung. Dieser Platz wird innerhalb der Europäischen Union von der Datenschutzgrundverordnung eingenommen. Aufgrund der verschiedenen Regelungen ist es nicht möglich, einheitliche Aussagen für den Datenschutz in den Vereinigten Staaten zu treffen, als logische Folge dieses Umstandes ist es ebenfalls nicht möglich, universell geltende technische Maßnahmen zu definieren, sollten diese angewandt werden müssen. Andere Szenarien, in welchen eDiscovery eingesetzt werden kann, sind aufgrund der fehlenden bundesstaatenübergreifenden Lösung kein Thema, beispielsweise die Datenschutzanfrage. Dafür betrachten wir hier die Anfragen der US-Geheimdienste. Abgesehen davon werden die gleichen Szenarien wie innerhalb der Europäischen Union betrachtet, da die tägliche Situation, in welchen Organisationen das Werkzeug eDiscovery einsetzen, unabhängig von ihrem geografischen Standort sind. Deshalb werden im Folgenden juristischen Prozesse mit und ohne Gerichtseinfluss betrachtet sowie interne Untersuchungen.

Im Folgenden wird nun vor allem der Grundsatz betrachtet, dass Unternehmen sich genau an die Regelungen halten müssen, welche sie sich selbst aufgelegt haben, da dies in der Mehrzahl der US-Bundesstaaten der Fall ist.

4.2.1 Juristischer Prozess mit Gerichtseinfluss (USA)

Die erste Möglichkeit, in welcher eDiscovery verwendet werden kann, ist ein Gerichtsprozess, in welchem das Gericht von einer Organisation fordert, bestimmte Dokumente, welche den Fall betreffen, freizugeben. Um ebenjene Dokumente innerhalb der Cloud der

Organisation zu finden, kann dabei eDiscovery verwendet werden. Technische Einschränkungen des Werkzeuges sind dabei nicht notwendig. Dies hat mehrere Gründe, zum einen, wenn die Organisation selbst keine Angaben zum Datenschutz gemacht hat, dann muss sie sich (in der überwiegenden Anzahl der Bundesstaaten) keine Gedanken über diesbezügliche Regelungen machen und kann so eDiscovery ohne Einschränkungen nutzen. Sollte es eine solche selbstauferlegte Regelung geben, welche besagt, dass die Organisation verschiedene Datenschutzregelungen hat, so kann das Gericht durch einen Durchsuchungsbeschluss noch immer diese Daten verlangen. Dies hat eine möglichst allumfassende Suche zur Folge, welche durch technische Einschränkungen behindert werden würde.

4.2.2 Juristischer Prozess ohne Gerichtseinfluss (USA)

Eine weitere Möglichkeit, um eDiscovery zu verwenden, ist der Wunsch der Organisation, bestimmte Indizien vor Gericht vorzulegen, welche ihren Standpunkt stützen. Ein Mittel, um diese Indizien aufzuspüren, ist das Verwenden des Werkzeugs eDiscovery in der Cloud der Organisation. Ob technische Einschränkungen umgesetzt werden, liegt wie erwähnt, in den meisten Bundesstaaten am Unternehmen selbst. Sollten das Unternehmen sich selbst diese Regelungen aufgesetzt haben, so muss beispielsweise die Erlaubnis von den Betroffenen eingeholt werden, wenn man eine Suche mit eDiscovery starten will. Als technische Einschränkung ist infolgedessen die Erstellung eines Filters notwendig, welcher alle Betroffenen umfasst, die dieser Verarbeitung ihrer Daten zugestimmt haben. Dafür ist ein Kopieren aller Daten der Betroffenen in einem gemeinsamen Ordner notwendig. Sollte es eine solche selbstauferlegte Regelung nicht geben, so sind auch keine Einschränkungen notwendig.

4.2.3 Interne Untersuchung: Katastrophenfall (USA)

Sollte ein Katastrophenfall innerhalb der Organisation auftreten, ist auch hier die Möglichkeit eDiscovery zu verwenden, gegeben. Durch die Nutzung des Werkzeugs kann beispielsweise nachvollzogen werden, wer welche Dokumente exportiert oder versendet hat. Einschränkungen bezüglich des Datenschutzes gibt es auch hier lediglich dann, wenn ein Unternehmen sich diese selbst auferlegt hat. Hierbei ist es allerdings unwahrscheinlich, dass es in ihren Datenschutzbestimmungen nicht dennoch verschiedene Regelungen implementiert hat, welche sie ermöglicht, auch in Situationen wie diesen personenbezogenen Daten zu verarbeiten. Durch das Zustimmen der Datenschutzerklärung akzeptiert man diese Art der Verarbeitung seiner personenbezogenen Daten. Auf der anderen Seite, wenn ein Unternehmen keine Angaben bezüglich des Datenschutzes macht, dann sind auch so keine technischen Einschränkungen, daher die Erstellung von Filtern erforderlich.

4.2.4 Interne Untersuchung: Mitarbeiterkritik (USA)

Die einzige große Besonderheit im Szenario von Mitarbeiterkritik ist das Vorhandensein der Mitarbeiter als Betroffene. Ansonsten ist das Prozedere meist gleich. Sollte die Organisation keine Angaben zum Datenschutz machen, ist die Verwendung von eDiscovery innerhalb der Organisation für solche Zwecke rechtens. Egal ob sie nun als Grund das Aufspüren von Diskriminierungserfahrungen hat oder ob mit ihr kontrolliert wird, was die Mitarbeiter über die Organisation kommunizieren. Sollten sie diese anders kommunizieren, daher Datenschutz gewährleisten wollen, ist diese Praxis nicht möglich.

4.2.5 Anfragen durch US-Geheimdienste

Ein neues Szenario, in welchem eDiscovery angewandt werden kann, ist das Anfragen oder besser gesagt Fordern von US-Geheimdiensten nach verschieden unter Umständen personenbezogenen Daten. Da dies aufgrund der verschiedensten Gesetze in den Kompetenzen der Nachrichtendienste liegt, hat hier auch der Datenschutz keinen Effekt. Abseits davon können sie über ein eigens dafür eingerichtetes, nicht öffentliches Gericht einen Durchsuchungsbefehl ausgestellt bekommen. In Folge dieser Umstände sind auch technische Einschränkungen des Werkzeugs eDiscovery nicht nötig oder zielführend.

5 Vergleich von Verwendungszwecken und Einschränkungen des Werkzeugs eDiscovery in der M365 Cloud

Durch die fortschreitende Globalisierung werden auch Organisationen immer internationaler und haben Standorte in den verschiedensten Ländern der Welt. Im Zuge dieser Verteilung der Organisationen über die ganze Welt ist auch die Betrachtung der jeweiligen Regelungen wichtig, um gesetzeskonform zu handeln. Ein Vergleich zwischen den Ländern bezüglich der Anwendbarkeit des Werkzeugs eDiscovery ist daher erforderlich.

5.1 Vergleich innerhalb der Europäischen Union

Innerhalb der Europäischen Union gibt es zunächst eine große Gemeinsamkeit, welche für die Anwendung von eDiscovery entscheidend sind und für die möglichen technischen Einschränkungen verantwortlich ist.

Diese Gemeinsamkeit ist die Datenschutzgrundverordnung, welche die Rahmenbedingung für den Datenschutz definiert. Durch die in der Verordnung geregelten Merkmale, welche den Datenschutz bestimmen, werden allen Organisationen, welche in der Europäischen Union wirken, genauen Regeln auferlegt, wie diese personenbezogenen Daten verarbeiten können und dürfen. Durch ihren Status als Verordnung gilt die DSGVO in allen Ländern der Europäischen Union sogar noch vor nationalem Recht. Einschränkungen und Abweichungen sind somit nicht in einem großen Maße möglich. Die Datenschutzgrundverordnung ist somit eine gemeinsame Grundlage für alle Länder innerhalb der Europäischen Union. Die Regelungen an Ansprüche sind somit, wenn nicht identischs so doch extrem ähnlich.

Als Unterschiede bestehen nun nationale Gesetze, welche die Datenschutzgrund-verordnung aber lediglich ergänzen können. Damit bildet diese mit ihren Regelungen und Grundsätzen noch immer die Basis für Datenschutz in der Europäischen Union.

Eine weitere Gemeinsamkeit sind dabei die verschiedenen Szenarien, in welchen eDiscovery von den Organisationen verwendet werden kann. Dies ist keine großen Überraschung, da die Standardvoraussetzung für Organisationen innerhalb der Europäischen Union gleich sind, somit sind auch ihre Anwendungsgebiete gleich.

Als Konsequenz dieser beiden Punkte gibt es innerhalb der Länder der Europäischen Union keine Abweichung bei der Anwendung von eDiscovery und damit verbundenen möglichen technischen Einschränkungen, um den Datenschutz zu gewährleisten. Durch die DSGVO und die standardmäßig gleiche Bedingung von Organisationen kommt es hierbei zu einer identischen Situation für alle Länder in der Europäischen Union.

5.2 Vergleich der Europäischen Union und den Vereinigten Staaten von Amerika

Bei der Gegenüberstellung der Vereinigten Staaten von Amerika und der Europäischen Union verhält es sich anders als bei dem Vergleich von Staaten innerhalb der Europäischen Union, in welcher es quasi keine nennenswerten Unterschiede gab. Dieser Sachverhalt ändert sich bei der jetzigen Gegenüberstellung. Nichtsdestotrotz gibt es auch hier einige Gemeinsamkeiten, welche beide in der Anwendung von eDiscovery besitzen, diese sind in Tabelle 1 dargestellt.

Tabelle 1: Gegenüberstellung EU und USA

Vergleichskriterium	Europäische Union	Vereinigte Staaten von Amerika
Verwendungszwecke	Juristische Anwendung (mit/ohne Gerichtseinfluss) Interne Untersuchungen Datenschutzanfragen nach DSGGVO	Juristische Anwendung (mit/ohne Gerichtseinfluss) Interne Untersuchungen Einsatz bei Anfragen von US-Geheimdiensten
Datenschutzrecht	Einheitlich geregelt in der Datenschutzgrundverordnung, ergänzende nationale Gesetz Nationen habe keine Möglichkeiten DSGVO zu umgehen	Keine nationale Regelungen Jeder Bundesstaat kann selbst entscheiden, mehrheitlich keine Regelung vorhanden
M365 Cloud und eDiscovery	Art und Weise der Nutzung ist gleich, keine Anpassung nach Kontinent	
Theorie des Datenschutzes	Allgemein in der Fachwelt gleiche Betrachtung der Grundsätze des Datenschutzes	

Als Erstes haben prinzipiell beide Vergleichsparteien, sowohl die Europäische Union als auch die Vereinigten Staaten von Amerika die gleichen Prinzipien und Grundsätze des Datenschutzes, gehen wir nur von der puren Definition dieses Begriffes aus und nicht von seiner praktischen Umsetzung. Diese Definition und damit verbundenen Normen sind in der allgemeinen Betrachtung grundsätzlich gleich. Ebenso gleich sind die verschiedenen, nicht durch Gesetze beeinflussten Szenarien, in welchen eDiscovery verwendet werden kann. Die Umstände in welchem die Anwendung von eDiscovery möglich ist, sind unabhängig von welchem Kontinent, auf welchem sich die Organisation befindet. Aufgrund dessen ähneln sich die Anwendungsgebiete sehr, sei es jetzt das Verwenden des Werkzeuges bei Gerichtsprozessen oder bei internen Untersuchungen.

Gleichzeitig gibt es hier auch einen Unterschied, namentlich die Datenschutzanfragen innerhalb der EU und die Einflussnahme der US-Geheimdienste. Diese müssen von allen Unternehmen in der Europäischen Union, durch den entsprechenden Artikel der Datenschutzgrundverordnung beantwortet werden. Etwas Vergleichbares wie die DSGVO gibt es in den Vereinigten Staaten nicht. Eine Grundlage für das Stellen und Beantworten solcher Anfragen ist also in den USA nicht vorhanden, die Praxis dieser Anfragen von Betroffenen existiert dort somit nicht. Dafür müssen sich alle Unternehmen innerhalb der Vereinigten Staaten den Anfragen der Geheimdienste beugen und dieses erfüllen. Eine vergleichbare Arbeitsweise ist innerhalb Europas ohne genaue Begründung der Nachrichtendienste und richterlichen Beschluss nicht möglich.

Dabei bietet die DSGVO noch weitere Unterschiede, sie bietet klare, verbindliche Regeln, welche Prinzipien ein Unternehmen erfüllen muss. Sie bietet Gesetze, welche personenbezogene Daten beschützen. In den Vereinigten Staaten ist so etwas nicht existent. Die Verbindlichkeit und Anforderung, Datenschutz zu gewährleisten, ist in den meisten Staaten nicht vorhanden. Hier entscheiden Unternehmen selbst, ob sie Datenschutz einhalten. Dies ist dabei aber auch keine absolute Entscheidung. Wenn sie Situationen definieren, in welchen sie personenbezogene Daten verarbeiten, so sind sie dazu in den meisten Bundesstaaten fähig, eDiscovery zu verwenden, auch wenn sie sagen, dass der Schutz von Daten von ihnen hohe Priorität hat.

Dies ist auch der größte Unterschied, wenn man die Seite der technischen Einschränkungen betrachtet, welche angewandt werden müssen, um eDiscovery als Werkzeug zu verwenden. Innerhalb der Europäischen Union gibt es dahingehend festgelegte Regelungen, wenn ein Werkzeug wie eDiscovery verwendet werden kann, um personenbezogene Daten zu verarbeiten. Abseits von diesen Regelungen gibt es verschiedene Prozedere, etwa die Einwilligung der Betroffenen, um personenbezogene Daten verarbeiten zu können. Diese Einwilligung kann auch auf eDiscovery erweitertet werden, bringt aber große organisatorische und technische Bürden mit sich, sollte man eDiscovery in dieser Situation verwenden. Untersagt ist beispielsweise das Verwenden von eDiscovery, um Mitarbeiter auszuspionieren oder anderweitig ohne Grund intern zu verwenden.

Dies ist in den meisten US-Bundesstaaten anders. Hier gibt es keine festgelegten Regelungen, keine Datenschutzgrundverordnung, welche für das gesamte Land gilt. Daraus folgen meist nicht existente Datenschutzbestimmungen und der Handlungsspielraum ist größer. Die Organisationen geben selbst an, wie die Daten verarbeitet werden. Daraus entsteht eine gewisse Willkür. Wenn die Organisationen eDiscovery für ihre internen Untersuchungen und das Überprüfen von Mitarbeitern verwenden wollen, so sind oft das einzige Hindernis sie selbst. Innerhalb der Europäischen Union muss dies überzeugend begründet werden, sollte eDiscovery dort eingesetzt werden. Dahingehend gibt es auch keine technischen Einschränkungen, die nötig sind, um personenbezogene Daten zu schützen. Sobald die Organisation in den USA beispielsweise in einer Erklärung beschreibt, dass personenbezogene Daten verarbeitet werden, um die Meinung der Mitarbeiter zu überprüfen, ist dies in den meisten Bundesstaaten der USA rechtens. Innerhalb der Europäischen Union ist dies anders, so gibt es zwar auch hier wenige Situationen, in welchen technischen Einschränkungen tatsächlich notwendig sind, um den Datenschutz zu gewährleisten. Der Grund für diesen Umstand ist allerdings, dass die Datenschutzgrundverordnung so exakte Regelungen aufstellt, in welchen das Werkzeug eDiscovery verwendet werden kann, dass Einschränkungen zum Gewährleisten des Datenschutzes nicht notwendig sind und eher der Effizienz dienen als sonst irgendeinem Zweck.

Alles in allem basiert der Unterschied der Vereinigten Staaten von Amerika und der Europäischen Union vor allem auf dem Vorhandensein (EU), bzw. den Nichtvorhandensein (USA) einer einheitlichen Datenschutzverordnung, welche für alle Länder sowie die einzelnen Bundesstaaten oder Verwaltungsdistrikte in diesen Ländern gilt.

6 Ergebnisse und Ausblick

6.1 Ergebnis und Diskussion

Im Zuge der Bachelorarbeit mit dem Titel „Ein Vergleich von nationalen und internationalen Verwendungsmöglichkeiten des Werkzeugs eDiscovery in der M365 Cloud und mögliche technische Einschränkungen zur Gewährleistung des Datenschutzes“ entstand eine Gegenüberstellung verschiedener, selbst gewählter Verwendungsmöglichkeiten im Bezug mit den Datenschutzbestimmungen einzelner Länder. Hierbei wurden auch verschiedene technische Einschränkungen betrachtet, welche unter Umständen zur Gewährleistung des Datenschutzes notwendig sind.

Dabei ist die Definition von Datenschutz an sich sehr einheitlich, es gibt in der Fachwelt wenig Diskussion darüber, welche Prinzipien erfüllt werden müssen, damit Datenschutz gewährleistet werden kann. Ebenso sind die verschiedenen Verwendungsmöglichkeiten für eDiscovery in Organisation sehr ähnlich. Es spielt hier keine große Rolle, ob eine Organisation nun in Europa oder in Nordamerika sitzt. Die Umstände und Gegebenheiten, in welchen eDiscovery verwendet werden kann, sind somit eigentlich identisch.

Die Unterschiede, welche sich nun doch zwischen den Vereinigten Staaten von Amerika und der Europäischen Union ergeben, sind letztlich im Grunde mit einem einfachen Punkt zu begründen. Dieser Punkt ist das Vorhandensein einer einheitlichen, für alle Staaten geltenden Datenschutzverordnung in der europäischen Union oder aber das Fehlen einer solchen in den Vereinigten Staaten von Amerika.

Im Falle der Europäischen Union und somit ihrer Mitgliedsstaaten und deren Bundesländer, gibt es einen einheitlichen Rahmen, welcher den Datenschutz regelt. Dieser ist die Datenschutzgrundverordnung, mit dieser werden Grundsätze und Bedingungen geschaffen, welchen sich alle Angehörigen der Europäischen Union beugen müssen. Gleichzeitig werden hier auch verschiedene Ausnahmen klar definiert, in welcher personenbezogene Daten verarbeitet werden. Es ist ein genaues Regelwerk mit einheitlichen Bestimmungen, deshalb sind auch innerhalb der Europäischen Union keine Unterschiede in der Verwendung von eDiscovery existent. Zum einen, weil es natürlicherweise, von Seite der Organisationen, immer gleichbleibende Situationen gibt, in welcher dieses Werkzeug verwendet werden kann und zum anderen, weil die DSGVO genaue Ausnahmen definiert, in welchen eDiscovery sonst noch verwendet werden kann, hier sei noch einmal das Prinzip der Datenschutzanfragen erwähnt.

Bei der Betrachtung der Vereinigten Staaten findet man keine einheitliche Datenschutzregelung. Vielmehr hat jeder Bundesstaat eigene Gesetze bezüglich des Datenschutzes. So gibt es auch einige, welche strengere Regelungen haben, aber der Großteil der einzelnen

Staaten besitzt keine nennenswerte Datenschutzregelung. Es wird vielmehr auf die Freiheit der Unternehmen und Verbraucher geachtet. Diese sollen selbst entscheiden, ob sie sich den Prinzipien des Datenschutzes unterwerfen. Infolgedessen kann es oft der Fall sein, dass Datenschutz in den Organisationen faktisch nicht existiert. Gleichzeitig gibt es vonseiten der US-Nachrichtendienste enormen Einfluss auf datenverarbeitende Organisationen. So gibt es ohne große Hürden hier die Möglichkeit, dass die Geheimdienste schnell an die verschiedensten personenbezogenen Daten kommen. In der Europäischen Union wäre so ein Vorgehen ohne ausführlich begründeten richterlichen Beschluss nicht denkbar.

Bemerkenswert in dieser Gegenüberstellung ist ebenfalls, dass technische Einschränkungen kaum notwendig sind, anders als die Fragestellung impliziert. So bietet die Datenschutzgrundverordnung verschiedene Ausnahmen, in welcher die Verarbeitung von personenbezogenen Daten legitim ist. Abseits davon ist es zwar möglich, durch die Zustimmung oder Ablehnung von einzelnen Personen die Nutzung von eDiscovery aufgrund von technischen Maßnahmen einzuschränken, wie realistisch solche Einschränkung bei immer größer werdenden Unternehmen sind, bleibt jedoch fraglich. Innerhalb der Vereinigten Staaten sind solche Einschränkungen meist eh nicht notwendig, sollte die Organisation ihre Datenschutzerklärung entsprechend gestaltet haben.

Wenn man nun den Vergleich mit einem einzigen Wort abschließen würde, so wäre dieses Wort wohl „Datenschutzgrundverordnung“. Wenn man es weiter betrachtet, kann man auch verschiedene Prinzipien hinter diesen unterschiedlichen Regelungen ausmachen. In der Europäischen Union gilt der Schutz der Person zunächst als höchstes Gut. Um dies zu beschützen, gibt es die Datenschutzgrundverordnung. In den Vereinigten Staaten steht nun weniger der Schutz des Menschen, sondern vielmehr der Schutz der Nation im Vordergrund, begründet durch die diversen Gesetze, welchen es den US-Nachrichtendiensten schnell und einfach erlauben, auf personenbezogene Daten zuzugreifen.

6.2 Selbstkritische Einschätzung

Im Rahmen der Bachelorarbeit wurde die Fragestellung der Arbeit und somit der Vergleich der Verwendungszwecke von eDiscovery beantwortet. Im Zuge dessen wurden verschiedene Grundlagen verständlich erklärt. Dabei reichten diese von technischen Voraussetzungen der Cloud und des Tools bis zur Vermittlung von Wissen über den Datenschutz als Idee bis hin zur Umsetzung dessen in verschiedenen Ländern.

Die Auswahl der verschiedenen Verwendungszwecke beruht dabei auf typischen Alltagssituation welche sich Organisationen ausgesetzt sehen. Die Erstellung des Vergleichs erwies sich als komplizierter als gedacht, da es herausfordernd war, verschiedene, klar voneinander abgrenzende Kategorien zu finden, welche im Vergleich verwendet werden konnten.

Trotz den Umständen war ein Vergleich möglich, welcher die Ursachen der Gemeinsamkeiten und Unterschiede der Verwendungszwecke des Werkzeugs eDiscovery klar gezeigt hat. Weniger ein Problem als vielmehr eine Überraschung stellte dabei die Gegebenheit dar, dass technische Einschränkungen zur Gewährleistung des Datenschutzes kaum notwendig waren, da durch rechtliche Bestimmungen die Verwendung und damit auch die datenschutzkonforme Nutzung klar umrissen ist.

6.3 Ausblick

Die Nutzung von Cloud-Diensten wird laut aktuellen Erkenntnissen weiterhin ansteigen, somit wird auch die Verwendung von eDiscovery wichtiger und wichtiger werden, unabhängig davon, in welcher Cloud [2]. Hierfür sind verschiedene Prozedere auf Seiten der Organisation zu erarbeiten, damit einem unrechtmäßigen Datenschutzverstoß (zumindest innerhalb der Europäischen Union) möglichst zuvorgekommen wird.

Besonders innerhalb der Europäischen Union sollte sich in Zukunft auch nach anderen Cloud-Anbietern umgesehen werden. So gilt zwar die Datenschutzgrundverordnung innerhalb der Europäischen Union, eine Einflussnahme von US-Geheimdiensten auf die Microsoft Cloud kann dennoch nicht ausgeschlossen werden. So warnen auch verschiedene Datenschutzverbände vor Nutzung dieser Cloud. Gleichzeitig gibt Microsoft selbst jedoch Hoffnung, beispielsweise weigert sich der Konzern gerade, personenbezogene Daten an US-Nachrichtendienste weiterzuleiten. Dieser Fall wird gerade vor einem US-Gericht verhandelt. Ein Restrisiko bleibt somit bestehen. [60]

Ideal wäre die Entwicklung einer Cloud innerhalb der Europäischen Union, welche bereits mit der Datenschutzgrundverordnung geplant wurde. Hier könnte man auch datenschutzkonforme Verarbeitung der Daten unabhängig der US-Geheimdienste gewährleisten.

Solange dies jedoch nicht existiert, ist eine Nutzung der M365 Cloud ohne echte Alternative. Innerhalb der Europäischen Union muss man sich stets des Datenschutzes bewusst sein und interne Prozesse gestalten. Ebenso muss man bereit sein, vor Gericht seine Entscheidung eDiscovery zu verwenden, und diese Entscheidung zu verteidigen. Innerhalb der Vereinigten Staaten wird sich an der Einflussnahme der Geheimdienste voraussichtlich nichts ändern: Ebenso wenig wie an der Situation mit dem Fehlen einer einheitlichen Datenschutzverordnung. Hier bleiben Veränderungen abzuwarten, eventuell werden mehre Bundesstaaten diesbezüglich Regelungen erlassen.

Literatur

[1] Statistisches Bundesamt. “Jedes dritte deutsche Unternehmen nutzte 2020 Cloud Computing.” https://www.destatis.de/DE/Presse/Pressemitteilungen/2021/05/PD21_241_52911.html (Zugriff am: 5. Aug. 2022).

[2] M. Ennemann, “Cloud-Computing im Höhenflug,” *KPMG*, 21 Jun., 2021. https://home.kpmg/de/de/home/themen/2021/06/cloud-computing-im-hoehenflug.html (Zugriff am: 5. Aug. 2022).

[3] Microsoft. “Microsoft Purview eDiscovery-Lösungen - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/ediscovery?view=o365-worldwide (Zugriff am: 5. Aug. 2022):

[4] Bundesamt für Sicherheit in der Informationstechnik. “Cloud Computing Grundlagen.” https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html (Zugriff am: 28. Jun. 2022).

[5] Microsoft. “Was ist die Cloud – Definition | Microsoft Azure.” https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-is-the-cloud/ (Zugriff am: 1. Jul. 2022).

[6] P. M. Mell und T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Gaithersburg, MD, 2011, doi: 10.6028/NIST.SP.800-145.

[7] Cloud Security Alliance. “The Definition of Cloud Computing | CSA.” https://cloudsecurityalliance.org/blog/2015/10/26/the-definition-of-cloud-computing/ (Zugriff am: 5. Aug. 2022)

[8] D. Lindner, P. Niebler und M. Wenzel, *Der Weg in die Cloud: Ein Leitfaden für Unternehmer und Entscheider* (Essentials). Wiesbaden, Heidelberg: Springer Gabler, 2020. Zugriff am: 4. Juli 2022. [Online]. Verfügbar unter: https://link.springer.com/content/pdf/10.1007/978-3-658-29101-3.pdf

[9] N. Antonopoulos und L. Gillam, *Cloud computing: Principles, systems and applications* (Computer Communications and Networks Ser). Cham: Springer International Publishing, 2017. Zugriff am: 6. Juli 2022. [Online]. Verfügbar unter: https://link.springer.com/content/pdf/10.1007/978-3-319-54645-2.pdf

[10] C. Surianarayanan und P. R. Chelliah, *Essentials of Cloud Computing*. Cham: Springer International Publishing, 2019.

[11] A. Kumawat, “Cloud Service Models (IaaS, SaaS, PaaS) + How Microsoft Office 365, Azure Fit In,” *CMSWire.com*, 10 Jul., 2013. https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php (Zugriff am: Jul. 11, 2022).

[12] Microsoft. “Microsoft Office gehört zu Microsoft 365 - Was ist neu?” https://www.microsoft.com/de-de/microsoft-365/microsoft-office (Zugriff am: 9. Jul. 2022).

[13] Microsoft. “Microsoft 365 – Abonnement für Office-Anwendungen | Microsoft 365.” https://www.microsoft.com/de-de/microsoft-365 (Zugriff am: 9. Jul. 2022).

[14] Microsoft. “Informationen zu Administratorrollen im Microsoft 365 Admin Center - Microsoft 365 admin.” https://docs.microsoft.com/de-de/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide (Zugriff am: 10. Jul. 2022).

[15] Microsoft. “Alle Microsoft 365-Pläne vergleichen (bisher Office 365) – Microsoft Store.” https://www.microsoft.com/de-de/microsoft-365/buy/compare-all-microsoft-365-products?market=de (Zugriff am: 11. Jul. 2022).

[16] Microsoft. “Microsoft 365 E3, E5 & F3 vergleichen | Microsoft Enterprise.” https://www.microsoft.com/de-de/microsoft-365/compare-microsoft-365-enterprise-plans?market=de (Zugriff am: 11. Jul. 2022).

[17] S. Attfield und A. Blandford, “Discovery-led refinement in e-discovery investigations: sensemaking, cognitive ergonomics and system design,” *Artif Intell Law*, Jg. 18, Nr. 4, S. 387–412, 2010. doi: 10.1007/s10506-010-9091-y. [Online]. Verfügbar unter: https://www.researchgate.net/profile/Simon-Attfield/publication/220539367_Discovery-led_refinement_in_e-discovery_investigations_Sensemaking_cognitive_ergonomics_and_system_design/links/552410430cf22e181e73877c/Discovery-led-refinement-in-e-discovery-investigations-Sensemaking-cognitive-ergonomics-and-system-design.pdf?origin=publication_detail

[18] Proofpoint. “Was ist eDiscovery und wie funktioniert es? | Proofpoint DE.” https://www.proofpoint.com/de/threat-reference/e-discovery (Zugriff am: 12. Jul. 2022).

[19] A. Taal, J. Le und J. A. Sherer, “A Consideration of eDiscovery Technologies for Internal Investigations,” in *Global security, safety and sustainability: Tomorrow´s challenges of cyber security ; 10th international conference, ICGS3 2015, London, UK, September 15 - 17, 2015 ; proceedings* (Communications in computer and information science 534), H. Jahankhani, A. Carlile, B. Akhgar, A. Taal, A. G. Hessami und A. Hosseinian-Far, Hg., Cham: Springer, 2015, S. 59–73.

[20] David Graus Zhaochun Ren Maarten De Rijke David Van Dijk Hans Henseler Nina Van Der Knaap, “Single and Multiple Entity Approaches to Linking,” [Online]. Verfügbar unter: http://users.umiacs.umd.edu/~oard/desi5/additional/Graus.pdf

[21] Michael Sperling†, Rong Jin, Illya Rayvych, Jianghong Li, and Jinfeng Y, “Similar Document Detection and Electronic Discovery: So Many Documents, So Little Time,” [Online]. Verfügbar unter: http://users.umiacs.umd.edu/~oard/desi5/research/Sperling-final.pdf

[22] Johannes C. Scholtes, “Comprehensive E-discovery and E-disclosure Technologies: Next-generation Deployment for Enterprise Search Tools,” 2006. [Online]. Verfügbar unter: https://taxonomystrategies.com/wp-content/uploads/2022/03/Enterprise-Search-April-2006.pdf

[23] EDRM. “EDRM Model - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/ (Zugriff am: 25. Jul. 2022).

[24] EDRM. “Identification Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/identification/ (Zugriff am: 26. Jul. 2022).

[25] EDRM. “Identification Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/identification/ (Zugriff am: 26. Jul. 2022).

[26] EDRM. “Preservation Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/preservation/ (Zugriff am: 26. Jul. 2022).

[27] EDRM. “Collection Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/collection/ (Zugriff am: 26. Jul. 2022).

[28] EDRM. “0.0 Introduction - EDRM.” https://edrm.net/wiki/introduction/ (Zugriff am: 27. Jul. 2022).

[29] EDRM. “Review Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/review-guide/ (Zugriff am: 27. Jul. 2022).

[30] EDRM. “Analysis Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/analysis/ (Zugriff am: 27. Jul. 2022).

[31] EDRM. “Production Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/production/ (Zugriff am: 27. Jul. 2022).

[32] EDRM. “Presentation Guide - EDRM.” https://edrm.net/resources/frameworks-and-standards/edrm-model/presentation-guid/ (Zugriff am: 28. Jul. 2022).

[33] Microsoft. “Erstellen und Verwalten von eDiscovery(Premium)-Fällen in Microsoft 365 - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/create-and-manage-advanced-ediscoveryv2-case?view=o365-worldwide (Zugriff am: 28. Jul. 2022).

[34] Microsoft. “Suchen nach Inhalten in einem eDiscovery-Fall (Standard) - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/search-for-content-in-core-ediscovery?view=o365-worldwide (Zugriff am: 29. Jul. 2022).

[35] Microsoft. “Erstellen und Ausführen einer Inhaltssuche im Microsoft Purview-Complianceportal - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/content-search?view=o365-worldwide (Zugriff am: 29. Jul. 2022).

[36] Microsoft. “Stichwortabfragen und Suchbedingungen für eDiscovery - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365-worldwide (Zugriff am: 29. Jul. 2022).

[37] Microsoft. “Anzeigen einer Vorschau von Ergebnissen eDiscovery-Suche - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/preview-ediscovery-search-results?view=o365-worldwide (Zugriff am: 30. Jul. 2022).

[38] Microsoft. “Anzeigen von Statistiken für eDiscovery-Suchergebnisse - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/view-keyword-statistics-for-content-search?view=o365-worldwide (Zugriff am: 30. Jul. 2022).

[39] Microsoft. “Einrichten von eDiscovery (Premium) in Microsoft Purview - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/get-started-with-advanced-ediscovery?view=o365-worldwide (Zugriff am: 1. Aug. 2022).

[40] Microsoft. “Zuweisen von eDiscovery-Berechtigungen im Microsoft Purview-Complianceportal - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide (Zugriff am: 1. Aug. 2022).

[41] CloudNine. “eDiscovery Technology Uses: Litigation, Investigations, Audits - CloudNine.” https://cloudnine.com/use-cases/ (Zugriff am: 2. Aug. 2022).

[42] P. Office, “Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Freund),” S. 47–194. Zugriff am: 6. September 2022. [Online]. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&qid=1662496561164&from=DE

[43] IBM. “IBM Documentation: Betriebssystem-Shells.” https://www.ibm.com/docs/de/aix/7.2?topic=administration-operating-system-shells (Zugriff am: 2. Aug. 2022).

[44] Microsoft. “Was ist PowerShell? - PowerShell.” https://docs.microsoft.com/de-de/powershell/scripting/overview?view=powershell-7.2 (Zugriff am: 3. Aug. 2022).

[45] Microsoft. “Einrichten von Compliancegrenzen für eDiscovery-Untersuchungen - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/set-up-compliance-boundaries?view=o365-worldwide (Zugriff am: 3. Aug. 2022).

[46] Microsoft. “Suchen Sie das Überwachungsprotokoll im Microsoft Purview Compliance Portal. - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide (Zugriff am: 4. Aug. 2022).

[47] Microsoft. “Microsoft 365-Warnungsrichtlinien - Microsoft 365 Compliance.” https://docs.microsoft.com/de-de/microsoft-365/compliance/alert-policies?view=o365-worldwide (Zugriff am: 4. Aug. 2022).

[48] R. Kneuper, *Datenschutz für Softwareentwicklung und IT: Eine praxisorientierte Einführung*. Berlin: Springer Vieweg, 2021. Zugriff am: 6. September 2022. [Online]. Verfügbar unter: https://link.springer.com/content/pdf/10.1007/978-3-662-63087-7.pdf

[49] International Organization for Standardization, “ISO/IEC 29100 E,”

[50] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. “Technische Anwendungen - Das Standard-Datenschutzmodell.” https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html (Zugriff am: 6. Aug. 2022).

[51] T. Klosowski, “The State of Consumer Data Privacy Laws in the US (And Why It Matters),” *The New York Times*, 06 Sep.a.m. ET, 2021a.m. ET. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ (Zugriff am: 6. Aug. 2022).

[52] International Association of Privacy Professionals. “State_Comp_Privacy_Law_Map.png (PNG-Grafik, 1200 × 675 Pixel) - Skaliert (80%).” https://iapp.org/media/images/resource_center/State_Comp_Privacy_Law_Map.png (Zugriff am: 7. Aug. 2022).

[53] Bureau of Justice Assistance. “The Foreign Intelligence Surveillance Act of 1978 (FISA) | Bureau of Justice Assistance.” https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286 (Zugriff am: 7. Aug. 2022).

[54] NSA, “fisa-court-exhibit-a,” [Online]. Verfügbar unter: https://netzpolitik.org/wp-upload/fisa-court-exhibit-a.pdf (Zugriff am: 8. Aug. 2022

[55] Bundestag, “US-Datenrecht,” [Online]. Verfügbar unter: https://www.bundestag.de/resource/blob/796102/ea53ffe8e08a9ab11e270719263d8c53/WD-3-181-20-pdf-data.pdf

[56] US Goverment, “Patriot Act,” [Online]. Verfügbar unter: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

[57] F. Online, “Hotmail, Outlook, Skype: Microsoft erlaubt NSA Zugriff auf Kundendaten,” *FOCUS online*, 12 Jul., 2013. https://www.focus.de/digital/computer/microsoft-erlaubt-

offenbar-zugriff-achtung-outlook-nutzer-die-nsa-kann-sie-ausspionieren_id_2925701.html (Zugriff am: 8. Aug. 2022).

[58] K. Foitzick, “Vom Patriot Act zum Freedom Act: Datenschutz in den USA,” *activeMind AG*, 07 Nov., 2015. https://www.activemind.de/magazin/freedom-act-datenschutz/ (Zugriff am: 8. Aug. 2022).

[59] T. Haar, “Wolkenbruch,” *Heise*, 27 Jun., 2018. https://www.heise.de/select/ix/2018/7/1530927567503187 (Zugriff am: 9. Aug. 2022).

[60] Regina Stoiber. “Ist bei Office 365 Datenschutz überhaupt möglich? | Datenbeschützerin Regina Stoiber.” https://regina-stoiber.com/2020/10/07/ist-bei-office-365-datenschutz-ueberhaupt-moeglich-microsoft-cloud-service-risiken-datenschutzkonform/ (Zugriff am: 9. Sep. 2022).

Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Mittweida, 12.09.2022	Niclas Wagner	
Ort, Datum	Vollständiger Name	Unterschrift

Nutzungs- und Verwertungsrechte

Ich übertrage zusätzliche Nutzungs- und Verwertungsrechte für die vorliegende Arbeit und allen damit in Zusammenhang stehenden Daten auf Grundlage der Creative Commons Lizenz "CC0" an alle genannten Betreuer dieser Arbeit.

Mittweida,12.09.2022
Ort, Datum