Microsoft Enterprise Onlinedienste

Einsatz unter Erfüllung von Compliance Anforderungen

Georg Weber
Strategie- & Technologieberater Großkunden | FSI Compliance
Microsoft Deutschland GmbH
georg.weber@Microsoft.com
+49 89 3176-3738

Microsoft

Agenda

1. Der deutsche Finanzsektor & Onlinedienste
2. Modell der geteilten Verantwortung in der Nutzung von Onlinediensten
3. Das Regionen-Prinzip und seine Bedeutung
4. Spezielle Ausrichtung auf Finanzdienstleister
5. (Risiko)Bewertung – Kontrolle – Prüfung
6. Management der Compliance als toolgestützter Selfservice
7. Onlinedienste & Datenschutz

Enterprise Onlinedienste & deutscher Finanzsektor

Wachsende Akzeptanz durch Kostenoptimierung, Schnelligkeit & Effizienz, höhere Sicherheit

→ "Cloud-Lösungen erscheinen aus heutiger Sicht sehr flexibel und zukunftsfähig… Datensicherheit geht vor und darf durch neue Lösungen nicht infrage gestellt werden - aber das wird sie nach meiner Einschätzung auch nicht."

Martin Zielke, Vorstandsvorsitzender, Commerzbank – Handelsblatt Online, 06.11.2017

→ „Clouds haben zwei Vorteile: Sie können helfen, Kosten zu senken. Und sie helfen uns, Prozesse zu vereinfachen und neue Anwendungen schneller an den Markt zu bringen. …“"Ich denke, dass mit der Zeit - wenn das Vertrauen in die Technologie wächst - mehr Dinge in öffentliche Clouds übertragen werden."

Pat Healey, CTO Infrastructure & Shared Technology Services, Deutsche Bank – Handelsblatt Online, 06.11.2017

→ „Es gibt keine weiteren Investitionen in neue on-premise Plattensysteme – wir investieren hier konsequent in Azure. Bis 2020 haben wir ein Rechenzentrum in unserer Zentrale abgebaut und durch Microsoft Azure ersetzt.“

Jürgen Schütz, Direktor & Bereichsleiter EDV, Provinzial Rheinland AG[1]

[1]: Siehe: https://customers.microsoft.com/en-us/story/provinzial-rheinland-azure-insurance-germany und https://customers.microsoft.com/en-us/story/provinzial-rheinland-azure-service-insurance-germany

Enterprise Onlinedienste & deutscher Finanzsektor

Wachsendes Verständnis & Akzeptanz der Aufsichten

- Intensiver Austausch innerhalb der Finanzbranche zu Onlinediensten als moderne Outsourcing Variante

- Aufsichten äußern sich öffentlich zur Nutzung von Enterprise Onlinediensten
  - "Da haben wir keine Restriktionen, wenn sichergestellt ist, dass die Daten in der Cloud richtig, verfügbar und sicher sind." …"Wir haben uns vorgenommen, unsere Outsourcing-Regeln im nächsten halben Jahr zu überprüfen…"

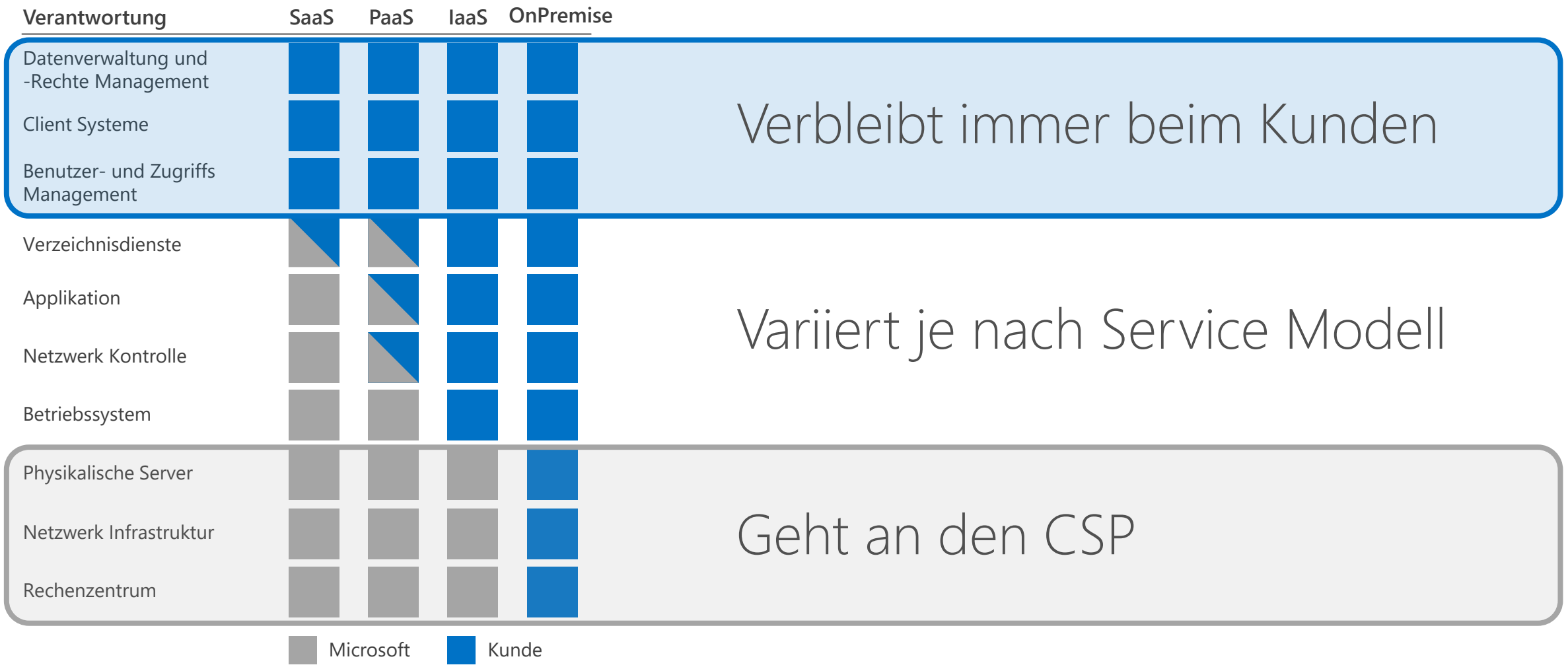
    Raimund Röseler, Exekutive Director / oberster Bankenaufseher, BaFin – Handelsblatt Nr. 213, S. 31, 06. November 2017

- Die „European Banking Authority" (EBA) verabschiedet erste Richtlinien zu Outsourcing an CSPs

- Weitere intensive Zusammenarbeit zw. Microsoft & Finanz Branche

Modell der geteilten Verantwortung

Drei wesentliche „Verantwortungszonen“



Regionen-Prinzip für lokalen Bezug

Hyper-Scale für Geschäftskunden – 42 Regionen weltweit (Stand: Q1/18) – (Ort)Vorgabe für lokale Nutzung

- 100+ Rechenzentren
- 20 Mio. Geschäftskunden weltweit
- ~95% der Fortune 500 & ~75% der DAX Kunden nutzen bereits Microsoft Enterprise Onlinedienste.

Geplant

* Betrieben von 21Vianet ** Daten Treuhand: Deutsche Telekom

Spezielle Ausrichtung auf Finanzdienstleister

Zusatzvereinbarung für Finanzdienstleistungsinstitute – orientiert an KWG, MaRisk, BAIT & EBA Anforderungen

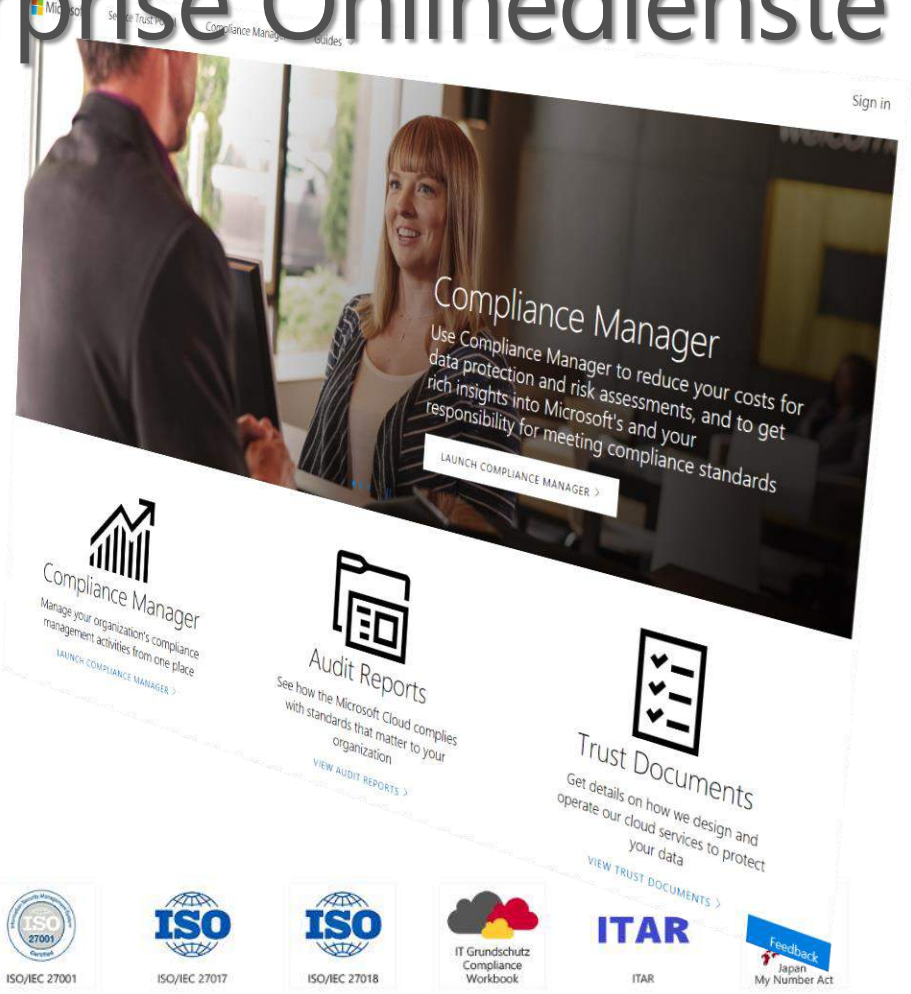
- Uneingeschränkter direkter Zugriff des Kunden auf seine Daten
- Uneingeschränkte Prüfungsrechte für die zuständige Finanzdienstleistungsaufsicht/Regulierungsbehörde
- Uneingeschränkte Prüfungsrechte für den Kunden und seine interne Revision & Prüfer im Rahmen der Mitgliedschaft im „FSI Compliance Program“ zzgl.:
  - Intensivem Informationsaustausch zw. Finanz Instituten & Microsoft - „Executive Committee“ als Organisationsorgan der Institute
  - Einflussnahme der Finanz Institute auf Compliance-relevante Anpassungen der Prüfungsumfänge
  - Regelmäßigen Penetration Tests
  - Benachrichtigung bei Ereignissen mit Auswirkung auf die Institute bzw. die Onlinedienste
  - Audit Webcasts und weitere Informations-Veranstaltungen
  - Bearbeitung von Supportfällen über vorhandenen Premier Support Vertrag
- Einsicht in Informationssicherheitsrichtlinien & andere sicherheitsrelevanten Praktiken & Richtlinien für jeden Online Dienst
- Microsoft verpflichtet sich zu
  - Durchführung von Prüfungen der Onlinedienste & Aushändigung der Prüfberichte
  - Kostenerstattung für Aufwände bei durch Microsoft zu vertretenden Sicherheitsvorfällen
  - Regelungen bei Insolvenz, Liquidation, Reorganisation über Unternehmen hinweg oder gesetzlichen / regulatorischen Auflagen

Bewertbarkeit der Microsoft Enterprise Onlinedienste

Einhaltung von & Zertifizierung nach internationalen Standards

- Regelmäßige Überprüfung nach internationalen Standards
  - Durch externe Prüfer & über die gesamte Dienstleistungskette
  - Aktuell 70 Zertifizierungen

- Umfassende & aktuelle Informationen dazu
  - Unter: https://servicetrust.microsoft.com/
  - Und im Kunden-Mandanten Portal



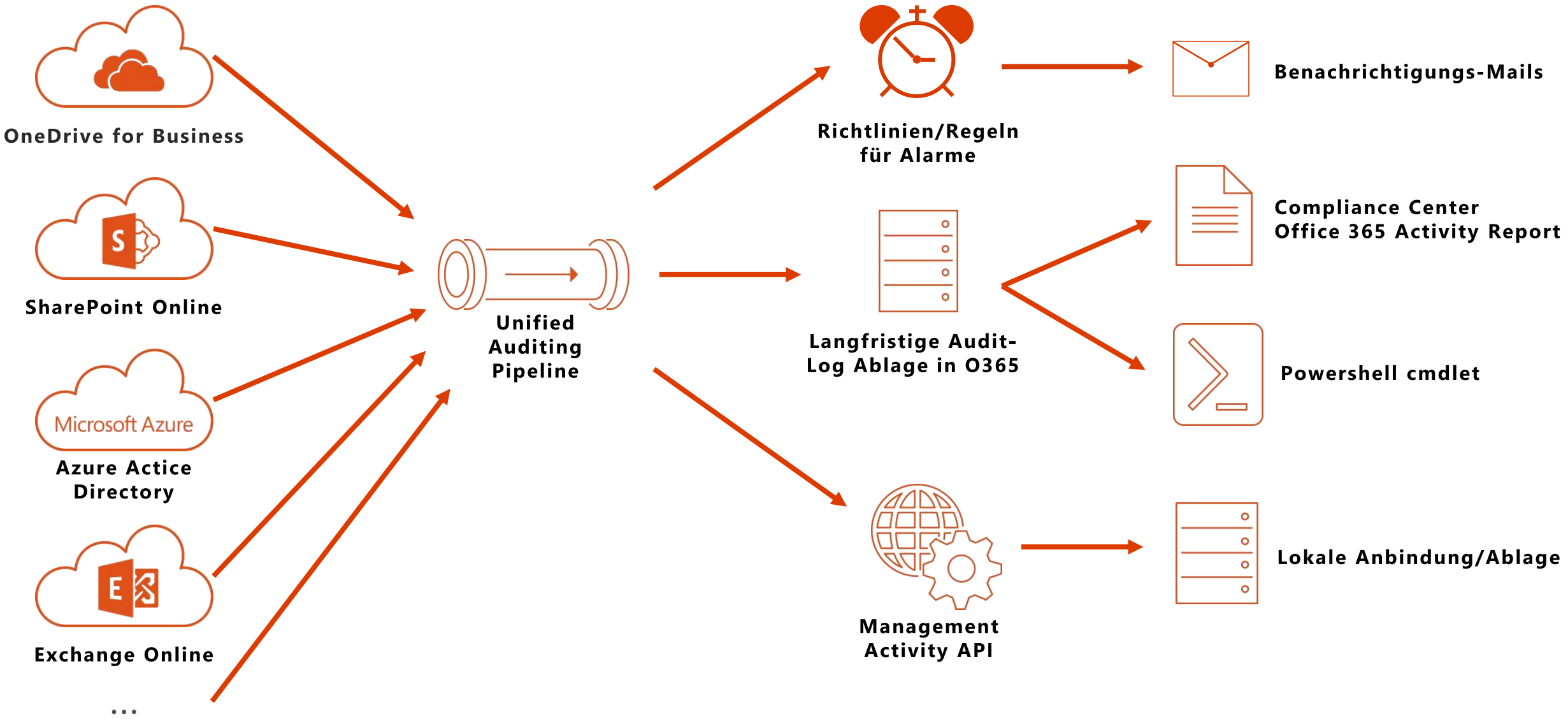
Argentina PDPA · Canadian Privacy Laws · CDSA · China GB 18030 · China MLPS · China TRUCS · CJIS · CSA CCM · IRS 1075 · ISO 22301 · ISO/IEC 27001 · ISO/IEC 27017 · ISO/IEC 27018 · IT Grundschutz Compliance Workbook · ITAR · Japan My Number Act

CS Mark (Gold) · DIACAP · DISA · ENISA IAF · EU Model Clauses · EU-U.S. Privacy Shield · FACT · FDA CFR Title 21 Part 11 · MARS-E · MPAA · MTCS · NIST 800-171 · NZCC Framework · PCI-DSS · Section 508 VPATs · SHARED ASSESSMENTS

FedRAMP · FERPA · FIPS 140-2 · FISC · FISMA · GxP · HIPAA/HITECH · IRAP (CCSL) · SOC 1 · SOC 2 · SOC 3 · Spain ENS · UK G-Cloud · HITRUST · India MeitY · IG Toolkit UK

Auditierungs- und Berichts Architektur

Real Time Auditierung – einheitliche Kontrolle für alle Dienste



Erfassen & verwalten sie den Grad ihrer Compliance

Management & Dokumentation

Ausgangssituation:

- Darstellung der Steuerungselementen (Controls) der genutzten Enterprise Onlinedienste in Bezug auf die für das Institut relevanten Vorschriften.

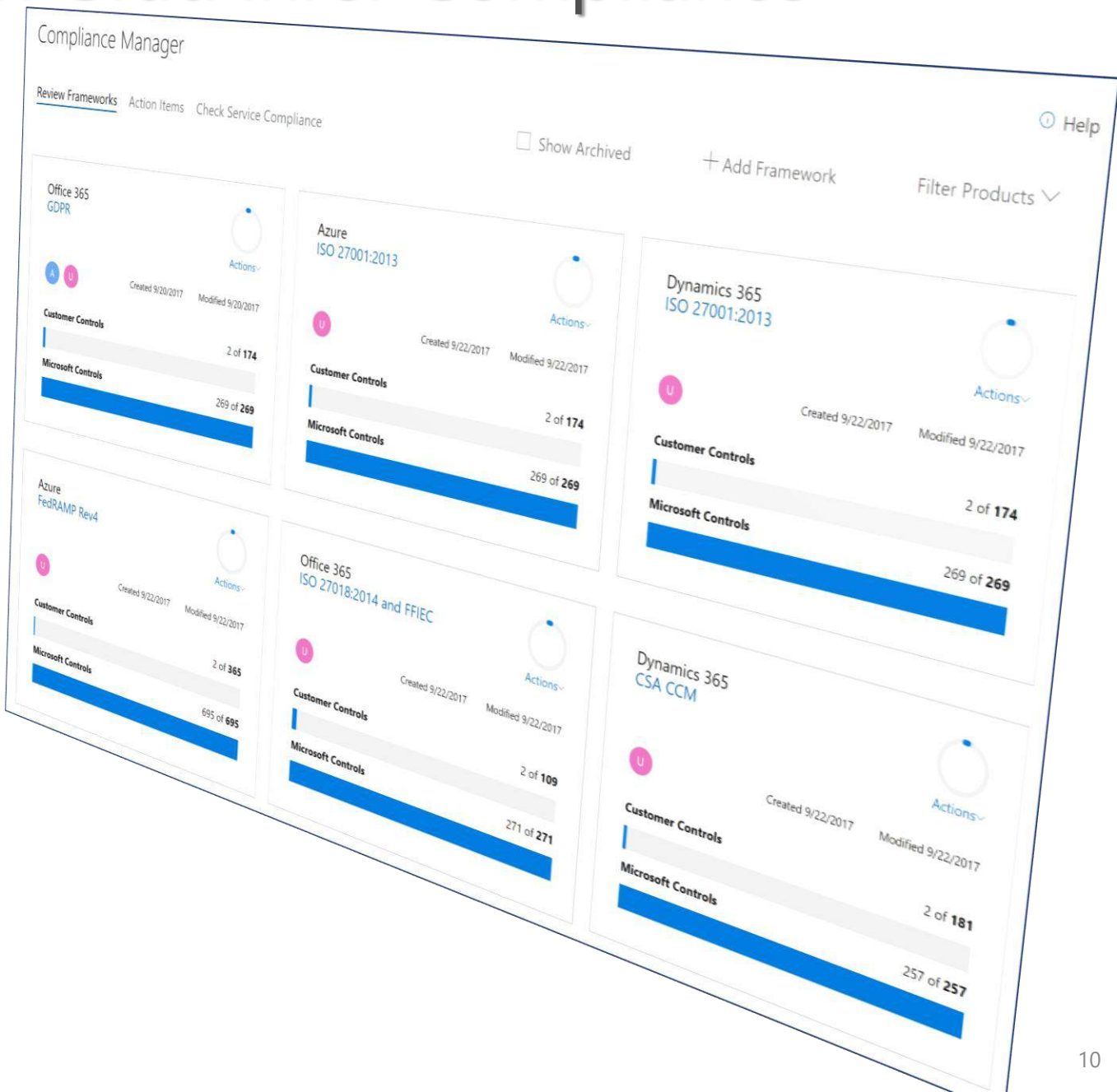
Prozesse & Ziel:

- Zentral verwaltete Transparenz über die Einhaltung der Compliance über alle Service-Modelle
  - SaaS (Office 365, Dynamics 365)
  - PaaS (Azure)
  - IaaS (Azure)

- End-to-End-Risiko- & Compliance-Ergebnisse, um die Konformität der Microsoft-Cloud-Assets mit den für das Institut relevanten Bestimmungen zu aggregieren/dokumentieren.

- Definition von Handlungsmaßnahmen & Verantwortlichkeiten.

- Belastbare Dokumentation der erreichten Compliance.



EXPORT TO EXCEL

Office 365 GDPR

Product	Framework	Compliant Controls		Assessed	Status	Last Modified
Office 365	GDPR	266/**443**	U	60%	NotStarted	9/25/2017

Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Customer Managed Controls

Office 365 Access Control Control Family

0/77 Assessed

MS Control	Certification Control(s)	Description	Assigned To	Status	Test Date	Test Result
AC-0100 Customer - 1 ...	GDPR:- Article 15(3)	The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	BG	Implemented	9/25/2017	Passed

Less

Necessary Customer Actions :

Implement Data Classification
Classify data with Labels for governance and to enforce policy (retention, disposition, etc.) based on that classification.

https://protection.office.com/#/tagslibrary

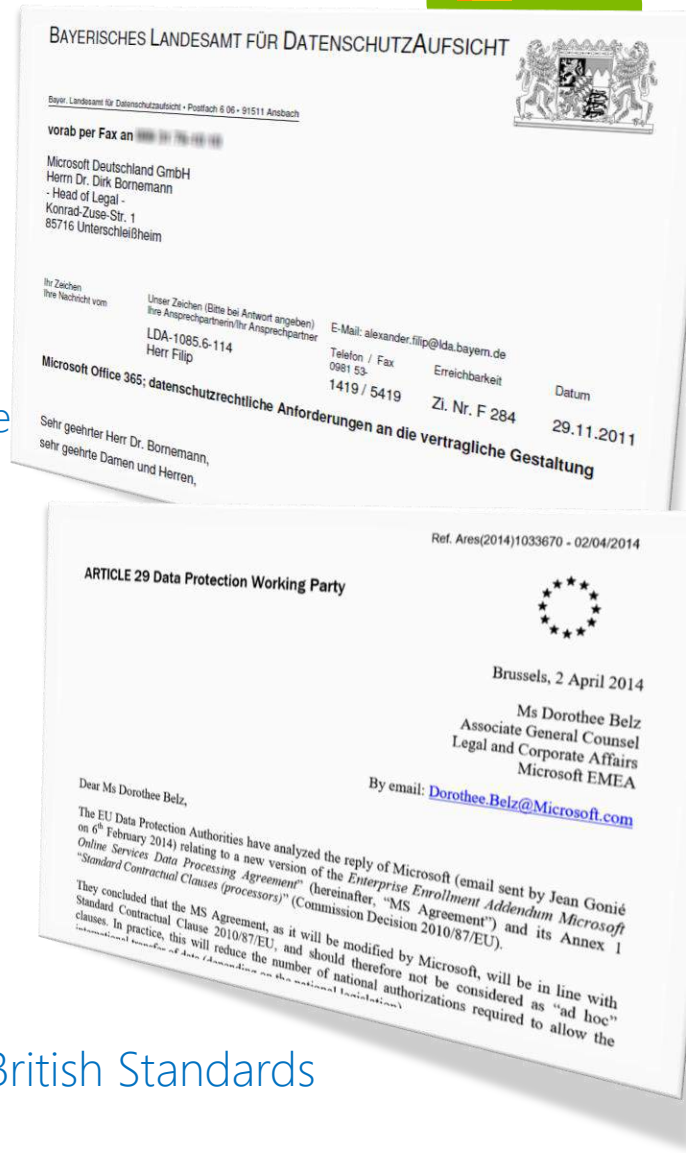
Execute Content Search
Use Content Search in the Security & Compliance Center to find content that's classified with a specific label in response to a specific data request (e.g. Data Subject, etc.)

Test Plan & Management Response :

1. Review business processes and workflow supporting data subject requests
2. Review data classification configuration to protect sensitive data subject to GDPR requirements.
3. Review content search performed to satisfy data subject requests.

Enterprise Onlinedienste & der Datenschutz

Vertragliche Vereinbarungen nach Kunden- & Marktbedarf & gem. geltender Vorgaben


BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

Bayer. Landesamt für Datenschutzaufsicht • Postfach 6 06 • 91511 Ansbach

vorab per Fax an

Microsoft Deutschland GmbH
Herrn Dr. Dirk Bornemann
- Head of Legal -
Konrad-Zuse-Str. 1
85716 Unterschleißheim

Ihr Zeichen, Ihre Nachricht vom | Unser Zeichen (Bitte bei Antwort angeben), Ihre Ansprechpartnerin/Ihr Ansprechpartner: LDA-1085.6-114, Herr Filip | E-Mail: alexander.filip@lda.bayern.de | Telefon / Fax: 0981 53-1419 / 5419 | Erreichbarkeit: Zi. Nr. F 284 | Datum: 29.11.2011

Microsoft Office 365; datenschutzrechtliche Anforderungen an die vertragliche Gestaltung

Sehr geehrter Herr Dr. Bornemann,
sehr geehrte Damen und Herren,

Ref. Ares(2014)1033670 - 02/04/2014

ARTICLE 29 Data Protection Working Party

Brussels, 2 April 2014

Ms Dorothee Belz
Associate General Counsel
Legal and Corporate Affairs
Microsoft EMEA

By email: Dorothee.Belz@Microsoft.com

Dear Ms Dorothee Belz,

The EU Data Protection Authorities have analyzed the reply of Microsoft (email sent by Jean Gonié on 6th February 2014) relating to a new version of the *Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement*" (hereinafter, "MS Agreement") and its Annex 1 "*Standard Contractual Clauses (processors)*" (Commission Decision 2010/87/EU).

They concluded that the MS Agreement, as it will be modified by Microsoft, will be in line with Standard Contractual Clause 2010/87/EU, and should therefore not be considered as "ad hoc" clauses. In practice, this will reduce the number of national authorizations required to allow the

- Vertrag zu Auftragsdatenverarbeitung (ADV) nach §11 BDSG und „EU Model Clauses“ als Rechtsgrundlage
  - 2011 Bestätigung durch „Bayerisches Landesamt für DatenschutzAufsicht“ (Office 365)
  - 2014 Anerkennung eines angemessenem Schutzniveaus durch die „Artikel 29 – Arbeitsgruppe
  - Microsoft zeichnet im August 2016 auch das „Privacy Shield“ Abkommen
- Keine Verwendung der Kundendaten zu Analyse-, Data Mining- oder Werbezwecken
- Kein direkter Zugriff durch Behörden oder Regierung auf Kundendaten & keine Unterstützung bei der Entschlüsselung von Kundendaten.
- Keine Herausgabe von Kundendaten ohne gültige gesetzliche Grundlage.
- Sourcecode Zugang (Transparenz Zentrum in Brüssel) und damit eine direkte Kontrolle möglich (z.B. durch BSI).
- Empfehlungen der „Cloud Security Alliance“ (CSA) und aus „Code of Practise“ nach „British Standards Institution“ (BSI) umgesetzt

Microsoft – EU-DSGVO Cloud-Relevanz & Regelungen

Relevante Punkte für Cloud-Angebote & deren Regelung

- Microsoft verarbeitet als Auftragsverarbeiter heute schon personenbezogene Daten
  - auf Weisung des Kunden
  - auf Basis eines Auftragsverarbeitungsvertrags
  - unter Einbezug der EU-Standardvertragsklauseln & Privacy Shield
- „Technisch organisatorischen Maßnahmen“ (TOMs) im geforderten Umfang[1]
- „Datenschutzfreundliche“ Nutzung bzw. „Privacy by Design“ & „Security by Design“
  - Z.B. Verschlüsselungs- und Pseudonymisierungsmöglichkeiten, Widerherstellungstechniken, versch. Prozess- und Sicherheitsbewertungen, etc.
- Handhabung von Unterauftragnehmern gem. den Anforderungen der DSGVO (vgl. Art. 28 Abs. 2 DSGVO)[2]
- IT-Sicherheit im Sinne der DSGVO-Anforderungen – Information & Unterstützung bei Ereignissen & Risiken
- Portal mit umfangreichen Informationen inkl. Tool zur Einschätzung
  - https://www.microsoft.com/de-de/trustcenter/privacy/GDPR und https://www.gdprbenchmark.com/DE/

[1]: Siehe: www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46
[2]: Siehe: www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46, S. 10 und Anhang 4, Seite 42, Punkt c

Verschlüsselung als Standard (erweiterbar)

Verschlüsselte Übertragung & Ablage – neben vielen anderen Sicherheitsfunktionen

- Verschlüsselung auf allen Zustands- und Kommunikationsebenen[1] – Schlüsselverwaltung durch Microsoft
  - Standard: (AES) 256-bit
  - Verschlüsselte Kommunikation
    - zw. den Rechenzentren
    - Zwischen Servern
    - Zwischen Client & Server
    - Mittels „Transport Layer Security" (SSL/TLS), 256-bit cipher (FIPS 140-2 Level 2-validiert)
  - Verschlüsselung „at rest":
    - Volume-/Disk-, dateibasierte Verschlüsselung
    - Mittels Microsoft BitLocker für Disk/Volume und granular (servicebasiert) für Mailboxen in Exchange Online und Dateien in SharePoint Online und OneDrive for Business
- Optionale Möglichkeiten:
  - S/MIME, PGP Email Verschlüsselung
  - Rechte Management (RMS bzw. „Azure Information Protection" (AIP)) auf Dateiebene.
    - Ermöglicht die „Handhabung" von verschlüsselten Dateien/Nachrichten (lesen, bearbeiten, weiterleiten, drucken, etc.)
    - Bis zu 45 Richtlinien, die einzeln aktiviert/deaktiviert werden können
    - Komplettes Lifecycle Management
  - „Customer Key" – zusätzliche Verwendung kundeneigener Schlüssel

[1] https://technet.microsoft.com/en-us/library/dn905447(v=office.15).aspx oder Whitepaper: „Content Encryption in Microsoft Office 356".

Erfüllung aufsichtsrechtlicher & gesetzlicher Anforderungen

Umsetzung und vertragliche Verpflichtung – eine Auswahl

- ✓ Eindeutige & detaillierte vertragliche Regelungen der Auftragsdatenverarbeitung
- ✓ Uneingeschränkte Informations-, Kontroll- und Prüfungsrechte für Aufsicht & Institut
- ✓ Nachvollziehbarkeit durch lückenlose Protokollierung & Dokumentation
- ✓ Gewissheit über Ort der Speicherung & Verarbeitung der Daten
- ✓ Löschen/endgültiges „Unkenntlich machen" der Kundendaten
- ✓ Datentrennung / Datenseparierung
- ✓ Transparenz & Kontrolle der Datenverarbeitung
- ✓ Garantierte Verfügbarkeit der Dienste & Daten
- ✓ Umsetzung der IT-Grundschutz Vorgaben des BSI
- ✓ Umfangreiche aktuelle Zertifizierungen wie ISO 27001 & 27018 & weitere
- ✓ Technisch Organisatorische Maßnahmen (TOMs) & rechtliche Rahmenbedingungen
- ✓ Umfangreiche beeinflussbare Sicherheitsmaßnahmen
- ✓ Beschränkter Zugriff auf personenbezogener Daten durch Drittstaaten