
lmbit

Bereiche, in denen wir uns auskennen

- Wir planen & implementieren die optimale Lösung für Sie. Auch nach einer Installation können Sie auf uns zählen:
  - Remote Unterstützung
  - Patch Management
  - Monitoring
  - Mitarbeiter-Schulungen
- Unsere Beratung erfolgt immer
  - ganzheitlich
  - unabhängig
  - transparent
  - branchenübergreifend

IT-Management

IT-Security

IT-Infrastruktur
& Cloud-Lösungen

Informationssicherheit

Service & Support

Allgemeine Leitsätze für SaaS / Cloud Produkte

- Es gibt NICHT „die EINE Lösung“
- Die Anbieter entwickeln sich laufend weiter
- Es wird darauf hinauslaufen, dass (Microsoft bis Ende 22 ?) sämtliche Daten in der EU gespeichert werden
- Aufsichtsbehörden argumentieren zumeist sehr pauschal
- Keine Berücksichtigung von möglichen Modifikationen oder Security Optimierungen
- Keine Differenzierung zwischen Verantwortlichkeit des Anbieters und Verantwortlichkeit des einsetzenden Unternehmens
- Keine Berücksichtigung der Lizenzmodelle und Zusatz-Software

Microsoft Time-Line

- Juli 20: „Schrems II“
  - MS nutzt nur noch SCC für Transfers
- Dezember 20: „Defending Your Data“
  - Commitment zur juristischen Anfechtung behördlicher Anordnungen
- September 21: „Neue SCC“
  - Erweiterung auf Produkte & Services (davor galt eine Trennung von Online Services)
- Mai 21: „EU Data Boundary“
  - Ankündigung zu Verarbeitung und Speicherung der Daten in der EU bis Ende 22

Transparenz und Vertrauen aufbauen

Answering Europe's Call: Storing and Processing EU Data in the EU

May 6, 2021 | Brad Smith - President and Chief Legal Officer

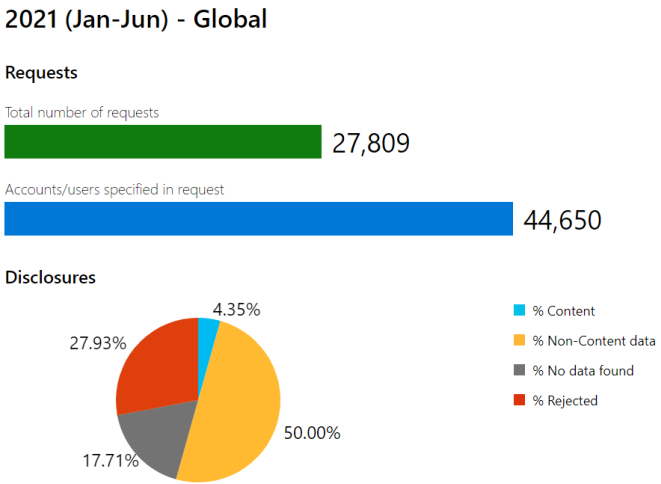
EU Data Boundary for the Microsoft Cloud: A progress report

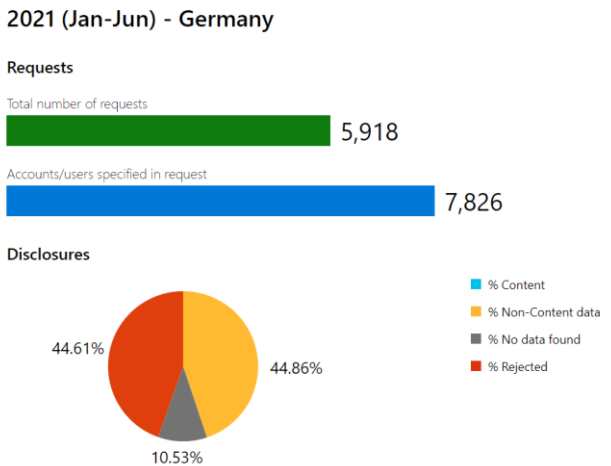
Dec 16, 2021 | Julie Brill, Corporate Vice President, Chief Privacy Officer, and Deputy General Counsel, Microsoft and Ralph Haupter, President Microsoft EMEA

Wie handelt Microsoft?

- CLOUD Act
  - Clarifying Lawfull Overseas Use of Data
  - Es wird immer zuerst an das betroffene Unternehmen verwiesen

- Law Enforcement Requests Report





Microsoft-Datenschutzbestimmungen

Privacy Shield-Abkommen zwischen der EU und den USA bzw. der Schweiz und den USA

Microsoft beachtet die Prinzipien des EU-U.S.- und des Swiss-U.S. Privacy Shield-Frameworks, betrachtet das EU-U.S. Privacy Shield-Framework allerdings aufgrund des Urteils des Europäischen Gerichtshofes in der Rechtssache C-311/18 nicht als legale Basis für die Übertragung persönlicher Daten. Weitere Informationen erhalten Sie unter weitere Informationen finden Sie auf der Privacy Shield-Website des U.S. Department of Commerce.

Kontakt

Wenn Sie Fragen oder Beschwerden zum Thema Datenschutz oder eine Frage an den Datenschutzbeauftragten von Microsoft haben (Microsoft Chief Privacy Officer oder EU Data Protection Officer), wenden Sie sich bitte unter Webformular an uns. Weitere Informationen zu Kontakten mit Microsoft, einschließlich Microsoft Ireland Operations Limited, finden Sie im Abschnitt So erreichen Sie uns dieser Datenschutzbestimmungen.

Auf dem Weg zur Compliance

1. Daten(Typen) Identifizieren
2. Transferwege identifizieren
3. Lokale und globale Bestimmungen identifizieren
4. Mögliche Maßnahmen bewerten
5. Maßnahmen treffen
6. Laufende Anpassungen durchführen

Damit müssen sich Unternehmen beschäftigen

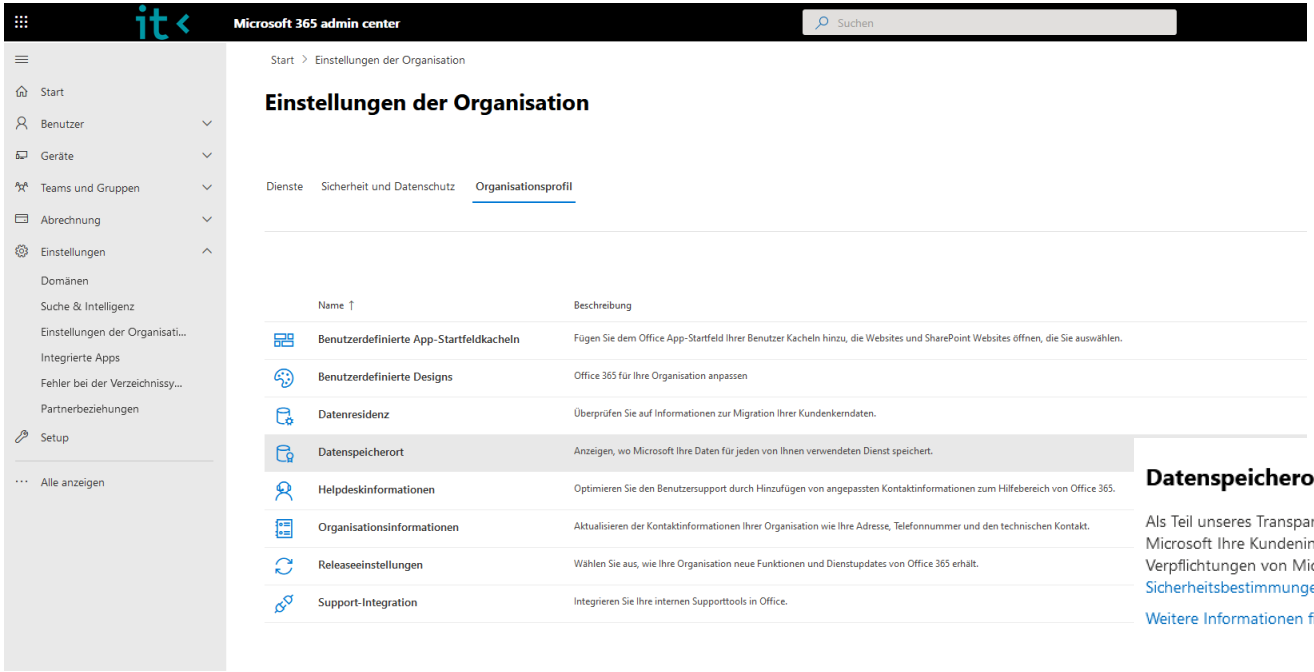
1. Wo befinden sich die Daten (Data Residence)
2. Welche Einstellungen wurden gesetzt
3. Welche Apps werden genutzt
4. Klassifizierung der Daten (Information Protection)
5. Verschlüsselung
6. Audits – Log Auswertung

→ Daraus resultieren die TOM's für ein Unternehmen

Sofort-Maßnahmen

- Prüfen Sie die Einstellungen Ihrer Organisation im MS 365 Admin Center
- Beschränken Sie die eingesetzten Apps auf ein Minimum
- Deaktivieren Sie Integrationen mit anderen Diensten (z.B. LinkedIn-Integration)
- Prüfen Sie die globalen Admins und reduzieren Sie diese
- Beschäftigen sie sich mit dem Compliance Center
- Beschäftigen Sie sich mit den Reports
- Aktivieren Sie ggf. Anonymisierungen in Reports
- Aktivieren Sie den Identitätsschutz (u.a. MFA)

Das MS 365 Admin Center



Datenspeicherort

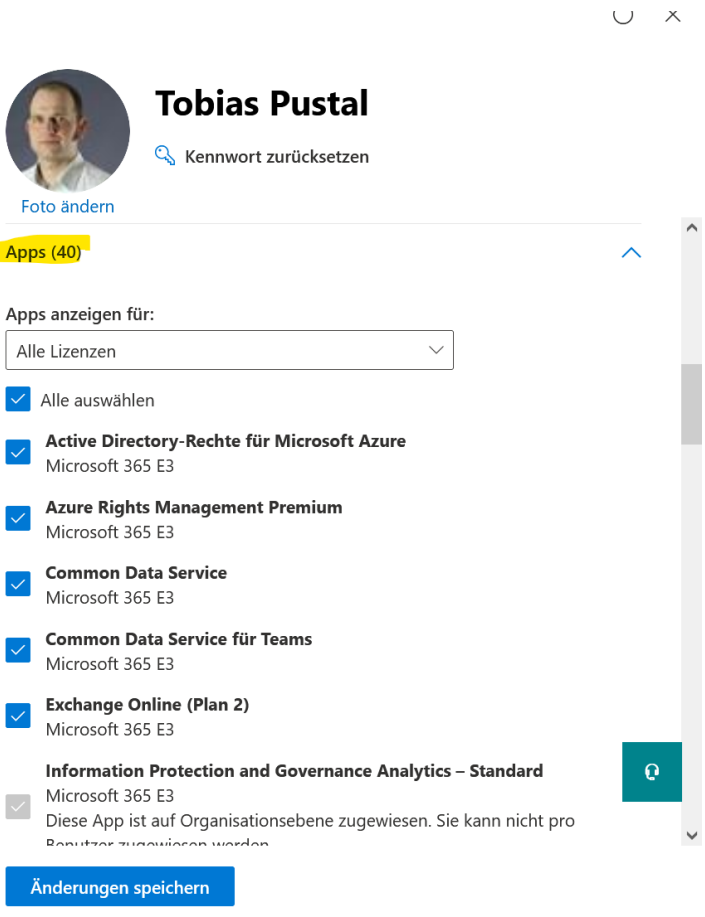
Als Teil unseres Transparenzprinzips veröffentlichen wir den Standort, an dem Microsoft Ihre Kundeninhalte speichert. Weitere Informationen zu den vertraglichen Verpflichtungen von Microsoft finden Sie in den Datenschutz- und Sicherheitsbestimmungen für Onlinedienste.

Weitere Informationen finden Sie im Office 365 Trust Center

Dienst	Ruhende Daten
Exchange	Europäische Union
SharePoint	Deutschland
Skype for Business	Europäische Union
Microsoft Teams	Deutschland

Näheres zu Anwendungen, die Sie nicht abonniert haben, finden Sie unter Wo sind meine Daten?.

Das MS 365 Admin Center



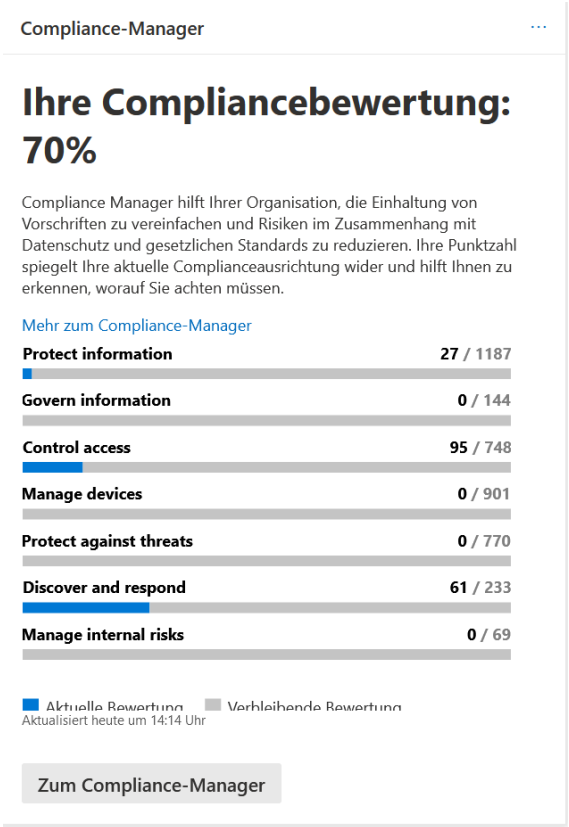
Weiterführenden Maßnahmen

- Arbeiten Sie mit Priviledged Access und Conditional Access
- Implementieren Sie Daten Klassifizierungen (Informationsschutz)
- Implementieren Sie Data Loss Prevention (DLP)
- Implementieren Sie Verschlüsselung (Customer Key, BYOK, HYOK, Double Key Encryption)
- Implementieren Sie Datenschutzmanagement (Microsoft Priva)
- Nutzen Sie ergänzende Produkte – z.B. 365 Total Protection (Hornetsecurity)

Beachten Sie, dass die meisten dieser Maßnahmen Einschränkungen bei den Benutzern verursachen und zusätzliche Lizenzen erfordern

Sprechen Sie daher unbedingt vorher mit einem Microsoft Experten

Microsoft 365 Compliance



Exkurs – Verschlüsselung

1. **Nutzung von Bordmitteln (Azure Key Vault, Priva)**

   Pro: moderater Implementationsaufwand, hohe Kompatibilität

   Contra: weitere Lizenzen erforderlich, Herstellerabhängigkeit

2. **Nutzung einer weiteren SaaS Lösung (HornetSecurity)**

   Pro: geringer Implementationsaufwand

   Contra: POC/Demo empfohlen, Herstellerabhängigkeit

3. **Nutzung eines Verschlüsselungsgateway (Thales, Eperi)**

   Pro: Multifunktional für unterschiedliche Cloud Services

   Contra: POC erforderlich, Einschränkung der Usability möglich

Exkurs – Verschlüsselung

ÜBERSICHT DER VERSCHLÜSSELUNGSMODELLE

Die folgende Tabelle fasst die Eigenschaften der beschriebenen Modelle bei korrekter Implementation zusammen.

Modell	Hold You Own Key	Double Key Encryption	Bring Your Own Encryption	Schlüsselverwaltung Cloudanbieter	Tokenisierung
Daten sind durch den Cloudanbieter lesbar	nein	nein	ja	ja	nein
Vollständige Cloud-Lösung	nein	nein	ja	ja	nein
Eigenes HSM erforderlich	ja	ja	ja*	nein	n.a.

* Die Schlüssel könnten auch ohne eigenes HSM erzeugt und anschliessend in die Cloud transferiert werden, dies würde aber deren Geheimhaltung stark beeinträchtigen.

Links

- https://privacy.microsoft.com/de-DE/privacystatement 
- https://aka.ms/dpa 
- https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?isToggleToList=True&lang=14 
- https://docs.microsoft.com/de-de/legal/gdpr
- https://docs.microsoft.com/de-de/compliance/regulatory/gdpr
- https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-action-plan
- https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-data-protection-impact-assessments

Herzlichen Dank !

- Tobias Pustal
  Teamleiter IT-Infrastruktur

  Fon +49 431 6703-124
  Tobias.Pustal@lmbit.de