Microsoft

Information GDPR Microsoft Teams

Friedhelm Peplowski

Michael Wirth
Stephanus

Aug-31

Was wird betrachtet und was nicht?

- **In diesem Dokument wird folgendes betrachtet:**
- Teams in einem europäischen Tenant und die dazu gehörige Datenhaltung
- Wie werden Daten in 1:1, 1:n und Teams verarbeitet und gespeichert

- **Was wird nicht betrachtet:**
- Microsoft Viva
- Telefonie via Teams

Beides wird aber in einer weiteren Version betrachtet!

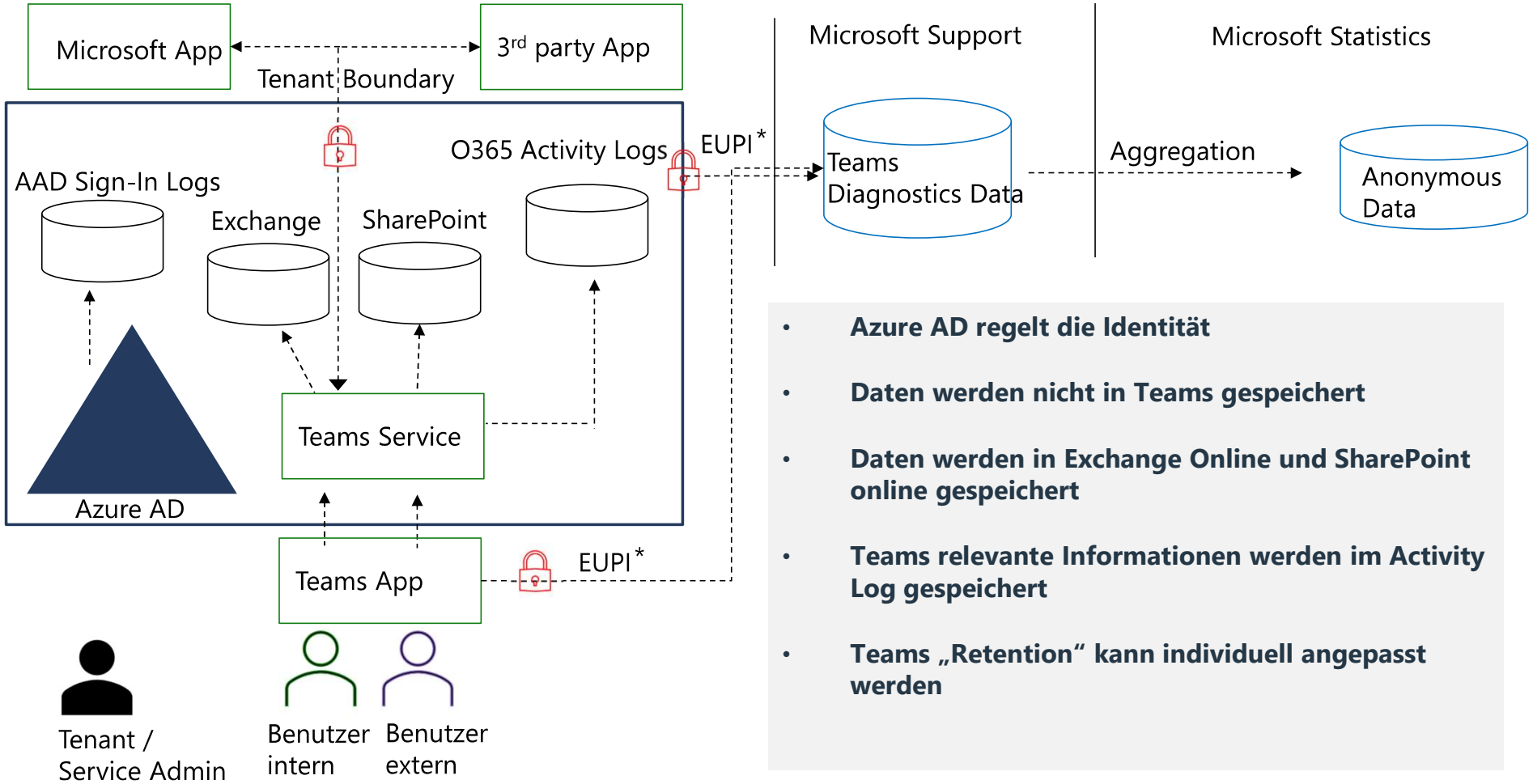
Generelle Information zu Teams

- Teams ist eine Kollaboration Plattform in Microsoft 365
- Teams kann für interne Nutzer, Gäste und externe Benutzer genutzt werden Azure Active Directory regelt die Identität.
- Microsoft Teams basiert auf Microsoft 365-Gruppen, Microsoft Graph und den Sicherheits-, Compliance- und Verwaltungsfunktionen in Microsoft 365
- Datenspeicherorte:
  - Chat = Exchange Online (individuelle Mailbox oder Gruppen Mailbox)
  - Files = SharePoint inkl. OneDrive for Business
- Die Administration ist sehr umfangreich und kann individuell angepasst werden
- Teams Aktivitäten werden von eDiscovery erfasst

ACHTUNG:
Bei Einsatz von Teams sollte über Datenklassifizierung, Data Loss Prevention und Kommunikation Compliance nachgedacht werden.

Dataflow Teams

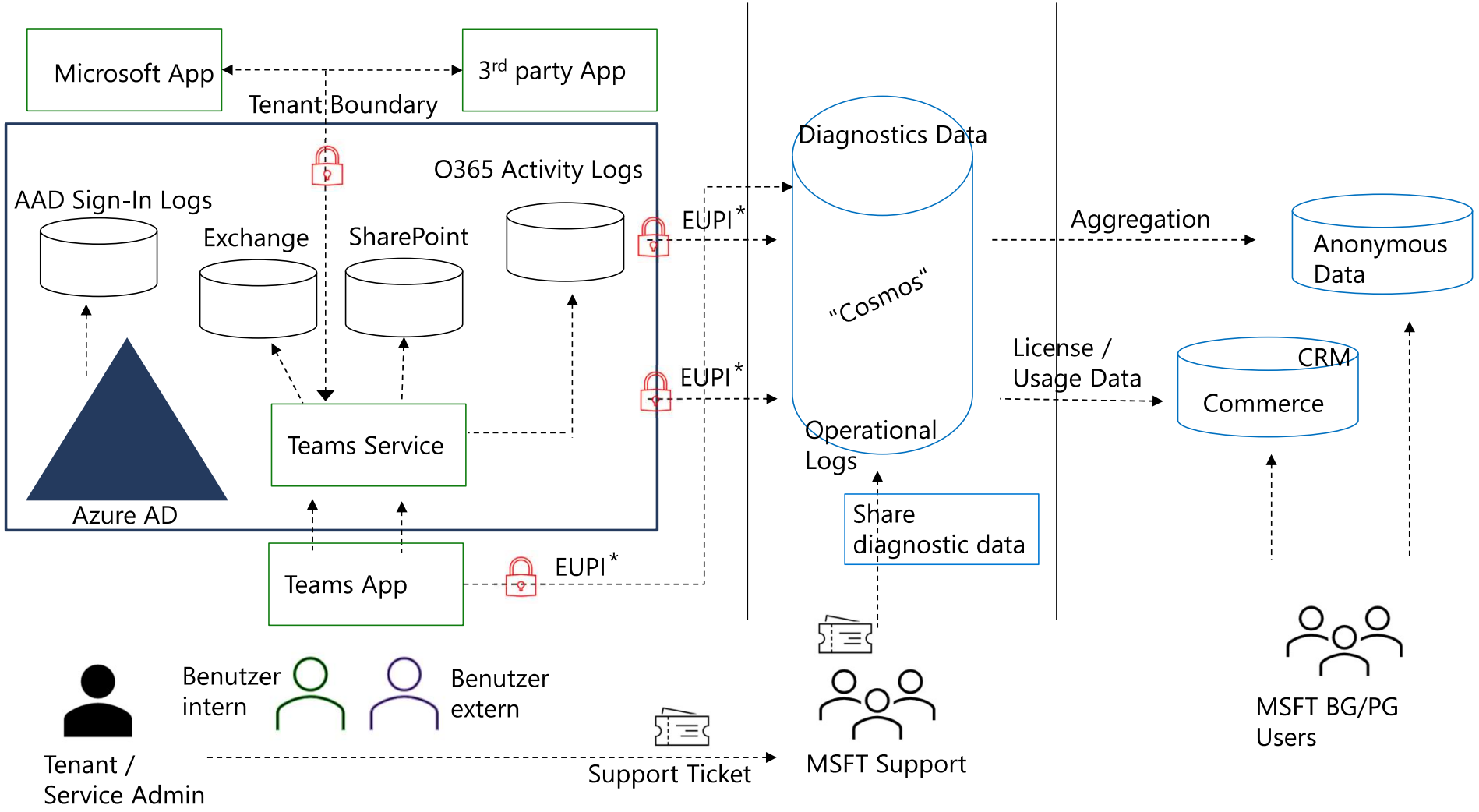
*EUPI = End User Pseudonymous Information



- **Azure AD regelt die Identität**
- **Daten werden nicht in Teams gespeichert**
- **Daten werden in Exchange Online und SharePoint online gespeichert**
- **Teams relevante Informationen werden im Activity Log gespeichert**
- **Teams „Retention“ kann individuell angepasst werden**

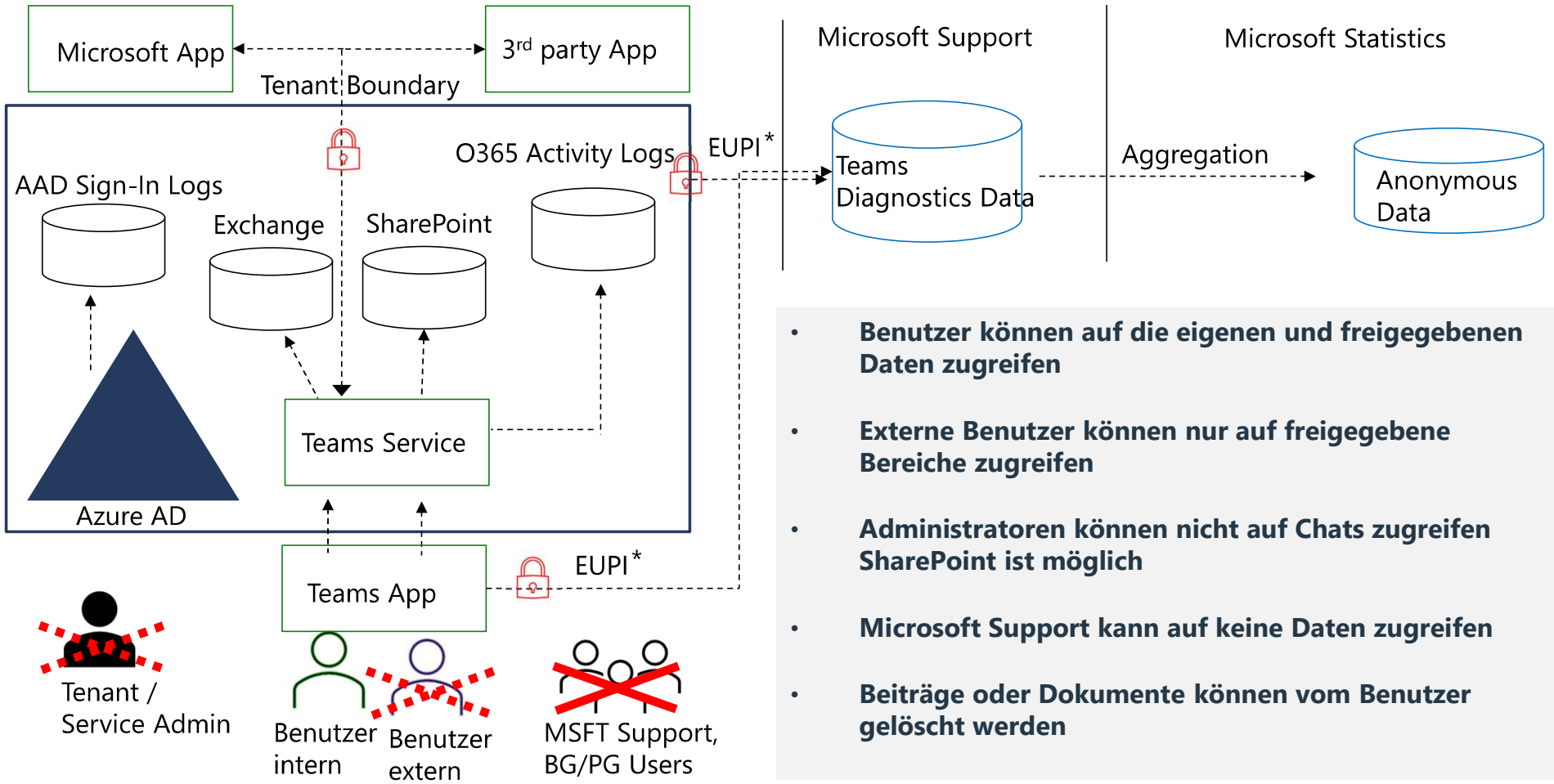
Dataflow Teams mit Support Ticket

*EUPI = End User Pseudonymous Information
Cosmos= Centralized repository where PII data is removed



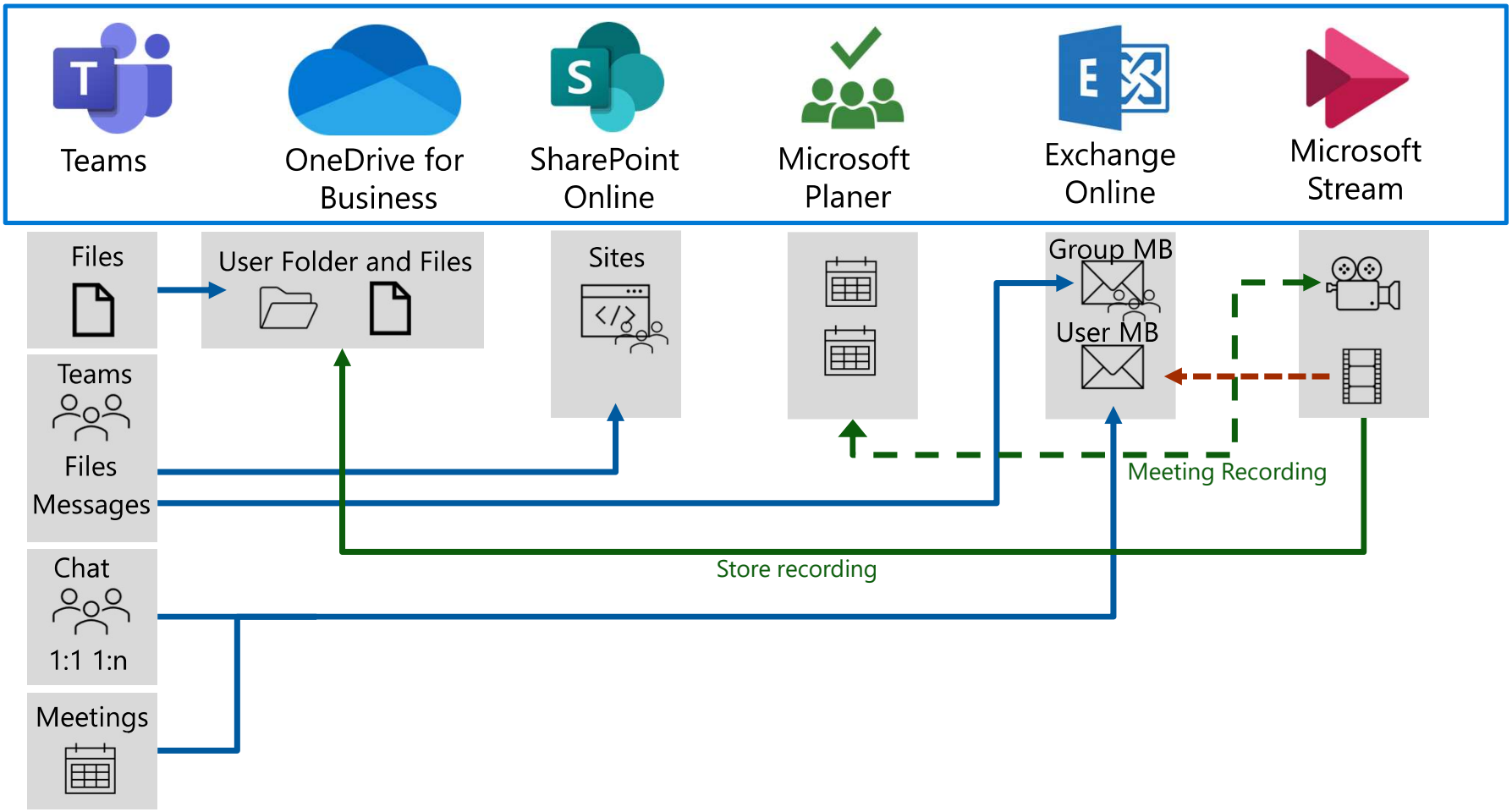
Data access Teams

*EUPI = End User Pseudonymous Information



- **Benutzer können auf die eigenen und freigegebenen Daten zugreifen**
- **Externe Benutzer können nur auf freigegebene Bereiche zugreifen**
- **Administratoren können nicht auf Chats zugreifen SharePoint ist möglich**
- **Microsoft Support kann auf keine Daten zugreifen**
- **Beiträge oder Dokumente können vom Benutzer gelöscht werden**

Vereinfachter Datenfluss mit Teams!



Was passiert wenn ein Team angelegt wird?

Ablauf:

1. **Es wird eine SharePoint Site angelegt**
2. **Es wird eine Gruppe im Azure AD erzeugt**
3. **Es wird eine Gruppen Mailbox erzeugt**
4. **Benutzer können Mitglied von beliebigen Gruppen sein**

Wo werden die durch Teams veröffentlichten Daten gespeichert?

- **Geographischer Speicherort (Geo Lokation):**

  Die Daten werden entsprechend der Lokation des Tenant in der jeweiligen Region gespeichert.

  - Bei einem Tenant in der EU werden die Daten in der EU gespeichert.
    https://admin.microsoft.com/AdminPortal/Home?#/Settings/OrganizationProfile/:/Settings/L1/DataLocationList

    Info:
    Bei einem 1:1 Chat aus verschiedenen geographischen Regionen werden die Chatnachrichten als auch die Attachments in der jeweiligen Region gespeichert. Hierzu später mehr über die Besonderheiten OneDrive.

- **Applikationsgebundener Speicherort:**

  In Teams generierte Daten werden in Exchange Online, SharePoint Online und OneDrive for Busienss gespeichert.

  Activity Logs werden innerhalb vom Tenant Boundary gespeichert.

  Support Logs werden im „Cosmos" außerhalb vom Tenant Boundary vorgehalten(Siehe Slide Dataflow Teams mit Support Ticket)

Wo werden Chat Daten mit Teams gleiche Lokation gespeichert?

- **1:1 oder 1:n Chat**

  Chat Nachrichten werden in der jeweiligen Benutzer Mailbox von Exchange online gespeichert.
  Die Nachrichten werden ähnlich einer E-Mail in der Mailbox mit einem speziellen Attribut gespeichert. Der Benutzer kann diese Nachrichten in Outlook **NICHT** einsehen

- **Attachments aus einem Chat:**

  Attachments werden in den jeweiligen den Benutzern zugehörigen OneDrive for Business gespeichert. Der Benutzer, der das Dokument hochgeladen hat behält die „Hoheit“ über das Dokument. Heißt, wenn der Benutzer das Dokument löscht so wird das Dokument auch bei dem oder die anderen Benutzer gelöscht.

Wo werden Chat Daten mit unterschiedlichen Lokationen gespeichert?

- **1:1 oder 1:n Chat**

  Chat Nachrichten werden in der jeweiligen Benutzer Mailbox von Exchange online gespeichert. Die Chat Nachrichten werden dann auch in unterschiedliche Lokationen gespeichert.

  Achtung: Die Nachrichten werden immer in beide Richtungen geschrieben. Heißt, wenn ein Benutzer eine Nachricht aus der EU an einen Empfänger außerhalb der EU sendet so wird diese Nachricht in der EU und in der anderen Lokation im Exchange Online gespeichert.

- **Attachments aus einem Chat:**

  Attachments werden in dem jeweiligen dem Benutzer zugehörigen OneDrive for Business gespeichert.

  Achtung: Das Attachment wird immer in beide Richtungen geschrieben. Heißt, wenn ein Benutzer eine Nachricht aus der EU an einen Empfänger außerhalb der EU sendet so wird diese Nachricht in der EU und in der anderen Lokation im OneDrive for Business gespeichert.
  Der Benutzer, der das Dokument hochgeladen hat behält die „Hoheit" über das Dokument.

Wo werden Team Nachrichten gespeichert?

- **Gruppen Chat**

  Chat Nachrichten werden in der dazugehörigen Gruppen Mailbox in Exchange online gespeichert.
  Auch gilt, die Nachrichten werden ähnlich einer E-Mail in der Mailbox mit einem speziellen Attribut in der Mailbox gespeichert. Der Benutzer kann diese Nachrichten in Outlook **NICHT** einsehen

- **Attachments oder Dokumente in einem Team:**

  Attachments oder Dokumente werden dazugehörigen SharePoint Site gespeichert. Abhängig von der Rechtevergabe kann entschieden werden wer Dokumente löschen

Wo werden Meeting Aufzeichnungen gespeichert?

- **Meeting Aufzeichnungen gleiche Lokation:**

  Aufzeichnungen eines Meetings (recording) werden in dem OneDrive des Benutzers gespeichert, der das Recording startet.

- **Meeting Aufzeichnungen unterschiedliche Lokation:**

  Aufzeichnungen eines Meetings (recording) werden in dem OneDrive des Benutzers gespeichert, der das Recording startet.

- Achtung: Wird die Aufzeichnung von einem Benutzer außerhalb der EU gestartet, so wird die Aufzeichnung außerhalb der EU gespeichert

Notwendige GDPR Aktivitäten von Kunden

- Microsoft stellt sicher, das die Daten mit Teams entsprechend der GDPR Vorgaben verarbeitet werden können.
- M365 Kunden müssen intern die GDPR Compliance durch geeignete Maßnahmen sicher stellen!
  - Benutzer informieren eventuell keine PII Daten ungesichert in Teams zu verarbeiten oder zu kommunizieren
  - Datenhaltung in einem Tenant in Europa ist gemäß GDPR möglich
    - Labeling, Verschlüsselung, Klassifizierung automatisch oder manuell, Data Loss Prevention, Insider Risk Management
  - Einrichten einer rollenbasierten Zugriffskontrolle RBAC.

Diese Information ist nur eine generelle Empfehlung und muss individuell an die Kundensituation angepasst werden. Es wird empfohlen diese Einstellungen mit dem Datenschutzbeauftragen zu besprechen.

GDPR Empfehlung für die Gruppen in Teams für lokale Datenhaltung?

- **Aus Sicht des Datenschutzes sollte der führende Tenant in der EU liegen**
- Aufzeichnungen für Meetings mit Teilnehmer aus unterschiedlichen Regionen sollten immer von einem Benutzer aus der EU gestartet werden. Eventuell Teams so administrieren, das nur der Organisator die Aufzeichnung starten kann.
- Schutz von PII Daten durch Label, Klassifizierung, Verschlüsselung und Data Loss Prevention
- Erstellen von Regeln für die Datenhaltung und mögliche Löschregelungen. (Retention)

Information Protection!

- **Teams ist eine Kollaborationsplattform und ermöglicht die interne wie externe Kommunikation**
- Mit Teams können Sensitive Daten (PII) übertragen oder ausgetauscht werden.
- Mit Teams könnten Interne vertrauliche Daten auch extern verteilt werden
- Via Teams kann unangebracht Sprache, unangebrachtes Verhalten und persönliche Beleidigungen Kommuniziert werden.

Für diese Fälle empfiehlt sich, Teams durch verschiedene präventive und reaktive Maßnahmen zu sichern.

Präventive Maßnahmen:
Labeling, Klassifizierung, Verschlüsselung und Data Loss Prävention

Reaktive Maßnahmen:
Insider Risk Management und Kommunikation Compliance

Wer kann auf Daten in Teams zugreifen?

- **Generell können nur die autorisierten Benutzer auf die jeweils freigegbenen Daten zugreifen.**
- Administratoren können bei entsprechender Berechtigung auf die jeweiligen SharePoint Seiten zugreifen. Jeder Zugriff wird im Activity Log aufgezeichnet und kann nachverfolgt werden.
- Administratoren können **nicht** auf die Chat Daten zugreifen mit Ausnahme eDiscovery.
  Im Rahmen eines eDiscovery Falles könnten auch andere Benutzer auf die Daten zugreifen.

  Dies erfordert das erstellen eines eDiscovery Case in Core eDiscovery oder Advanced eDiscovery.
  Alle Aktivitäten im Bereich eDiscovery werden geloggt und sind nachvollziehbar.
- Microsoft Support nicht auf die Daten zugreifen! Ein Zugriff ist nur mit Genehmigung durch den Kunden möglich und kann mit Customer LockBox zusätzlich gesichert werden.
- **ACHTUNG:**
  Einschränken und kontrollierte vergabe der Rechte durch Rollenbasiertes Zugriffssteuerungsmodell (RBAC) empfohlen!

Rollenbasiertes Zugriffssteuerungsmodell (RBAC)

- **ACHTUNG:**
  Berechtigungen im Security & Compliance Center überprüfen.
- Berechtigungen im Security & Compliance Center basieren auf dem Rollenbasierten Zugriffssteuerungsmodell (RBAC).
- Exchange Rollengruppen sind nicht identisch mit den Compliance Rollengruppen diese müssen separat betrachtet und angelegt werden.
- Der Zugriff auf Information durch Administratoren sollte so im Compliance Center eingeschränkt werden!
- Es gibt eine Vielzahl von Rechten für die granulare Vergabe der jeweils benötigten Rechte

Quelle: Berechtigungen – Security & Compliance Center - Office 365 | Microsoft Docs

Wie werden die Daten in Teams sicher verarbeitet?

- **Datensicherheit:**
  Alle Daten werden verschlüsselt übertragen.
  Ein Administrator des Tenant hat **keinen** Zugriff auf Chat Daten.
  Microsoft Support hat keinen Zugriff auf die Daten.

- **Vorhaltezeit:**
  Alle Daten werden gemäß den Vorgaben durch den Kunden vorgehalten. Eine Retention Policy muss entsprechend definiert werden.

- **Daten löschen:**
  Benutzer können Chat Nachrichten und Dokumente löschen.
  Daten können automatisch entsprechend der Vorhaltezeit gelöscht werden.

Benutzer Aktivitätsbericht Teams?

- Benutzer Aktivitätsbericht
- Benutzer Aktivitätsbericht Teams:
  Microsoft Teams – Benutzeraktivitätsbericht - Microsoft Teams | Microsoft Docs
  - Der Benutzer Aktivitätsbericht ist sehr umfangreich und kann aus GDPR und Betriebsrat Sicht kritisch bewertet werden.
  - Der Aktivitätsbericht kann anonymisiert werden.
- **Mit dem Aktivitätsbericht kann erkannt werden, wie aktiv ein Benutzer ist. Es können aber hieraus keine Schlüsse, auf die Datenverarbeitung oder die Daten gezogen werden.**

Was wird für den Microsoft Support für Teams geloggt?

- Für Service Zwecke werden ausschließlich Aktivitäten geloggt.
  - Für interne Benutzer eine GUID übertragen aber kein Name oder UPN, der Support kann die GUID nicht nachverfolgen.
    Dies kann nur durch den Admin der Organisation erfolgen!
    EUPI = End User Pseudonymous Information
  - Aktivitäten externe Benutzer werden pseudonymisiert. Eine Nachverfolgung durch den Support ist nicht möglich.
  - Die Logeinträge werden bis zu 180 Tage aufbewahrt und danach gelöscht
- Logs für Statistiken
  - Es werden Statistikdaten erfasst um eine Überblick über Nutzung von Teams zu erhalten.
  - Es werden **keine** PII Daten oder Daten erfasst die auf einen Benutzer und oder Tenant zurückverfolgt werden können.

Zusatzinformation zu Protokolldaten „Cosmos“

- Zusätzliche Protokolldaten für Microsoft Techniker
  - Verschiedene Arten von Protokolldaten werden von Microsoft 365 Servern in eine proprietäre Lösung für die Sicherheitsüberwachung für die Analyse in einen internen Big Data Computing-Dienst (Cosmos) für die langfristige Speicherung hochgeladen.
    Diese Datenübertragung erfolgt über eine FIPS 140-2-validierte TLS-Verbindung an genehmigten Ports und Protokollen mithilfe eines proprietären Automatisierungstools namens Office Data Loader (ODL).
  - Vor dem Hochladen verwendet die ODL-Anwendung einen Scrubbing-Dienst, um alle Felder zu entfernen, die Kundendaten enthalten, z. B. Mandanteninformationen und Informationen zur Identifizierung von Endbenutzern, und diese Felder durch einen Hashwert zu ersetzen.
- Zugriff auf die Protokolldaten
  - Der Zugriff auf Microsoft 365 in Cosmos gespeicherten Daten ist auf autorisiertes Personal beschränkt. Microsoft schränkt die Verwaltung von Überwachungsprotokollen auf eine begrenzte Teilmenge der Sicherheitsteammitglieder ein, die für die Überwachungsfunktionen verantwortlich sind.
  - Das Sicherheitsteam hat keinen ständigen administrativen Zugriff auf Cosmos, und alle Änderungen werden aufgezeichnet und überwacht.

Quelle: [Microsoft 365 interne Protokollierung für Microsoft 365 Engineering - Microsoft Service Assurance | Microsoft Docs]