Compliance mit IT

Datenmanagement im Kontext Compliance



Jens Lorenz
Strategic Consultant, CISSP, CCSP, CIPT
Swiss IT Security Deutschland GmbH

Aktuelle Problemstellungen

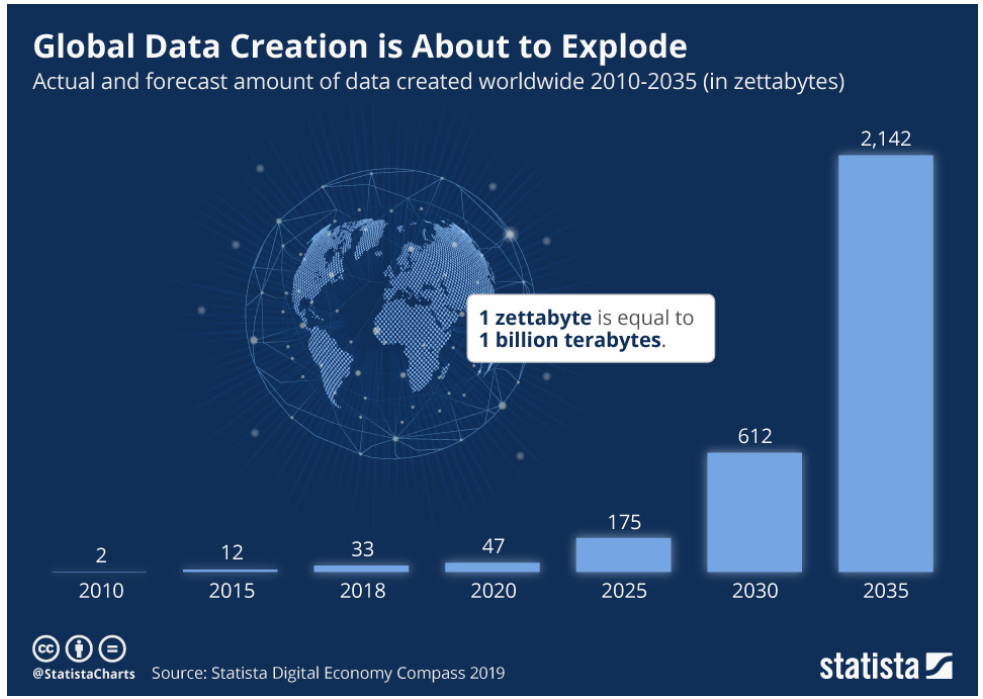
Digitalisierung von Fachdaten und regulierten Daten

- Unstrukturierte Datenablage und Verarbeitung in Office Anwendungen
  - Kollaboration über Unternehmensgrenzen
    - MS Teams, E-Mail, Dateifreigaben etc.
- Kunden und Partner nutzen stärker digitale Kommunikation
  - Oftmals immer noch kein „offiziellen“ Kommunikationswege
  - Paradigmenwechsel auch durch den Generationswechsel

Aktuelle Problemstellungen

Exponentieller Datenzuwachs durch die Digitalisierung

- „Klassische“ Methoden von Datenmanagement sind oft unzureichend
- Compliance-Anforderungen nehmen zu
  - Geschäftskontinuität
  - Informationssicherheit
  - Datenschutz



Quelle: Chart: Global Data Creation is About to Explode | Statista

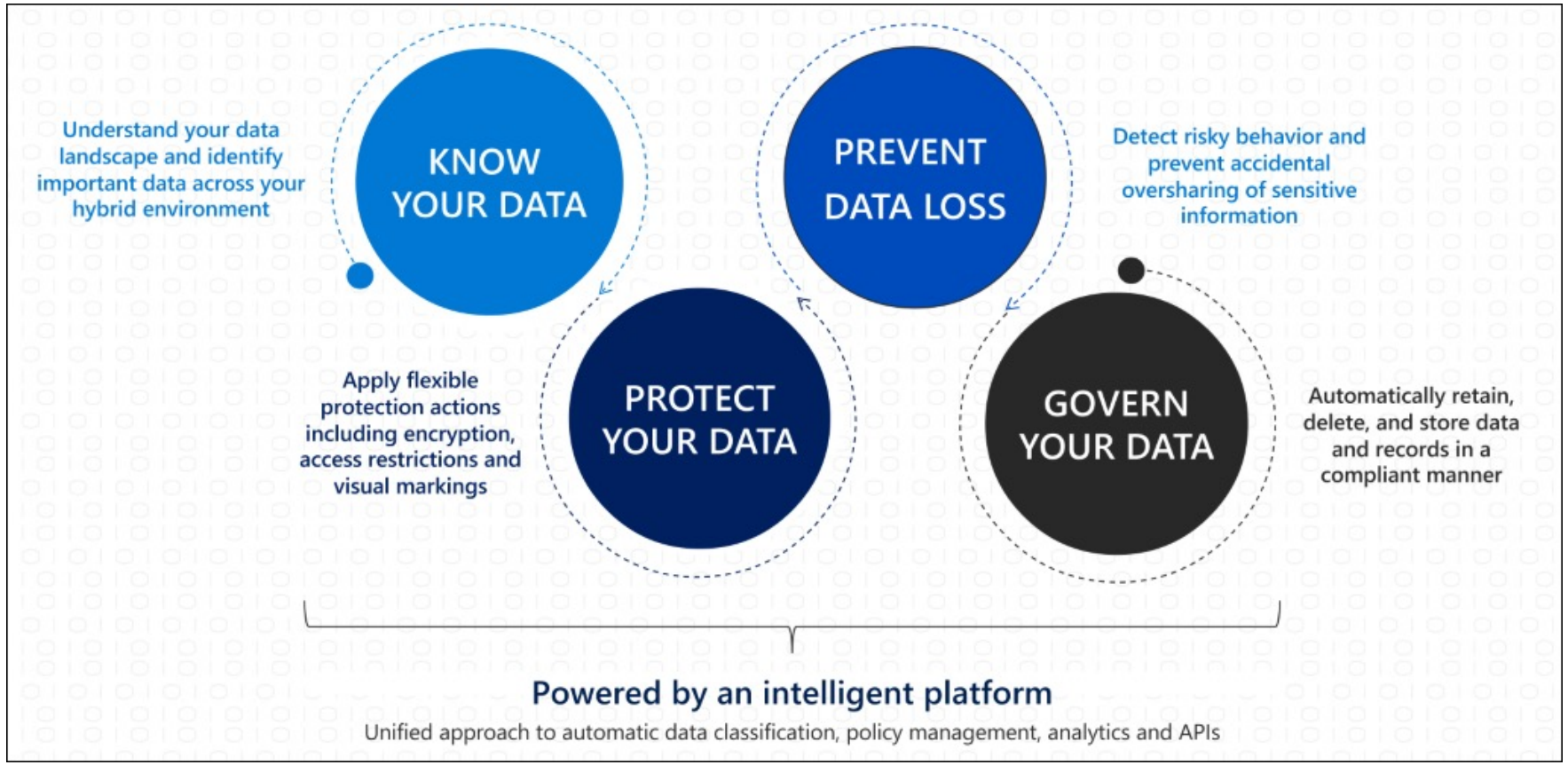
Das Spannungsfeld



Datenmanagement mit Microsoft 365

Microsoft Information Protection & Governance

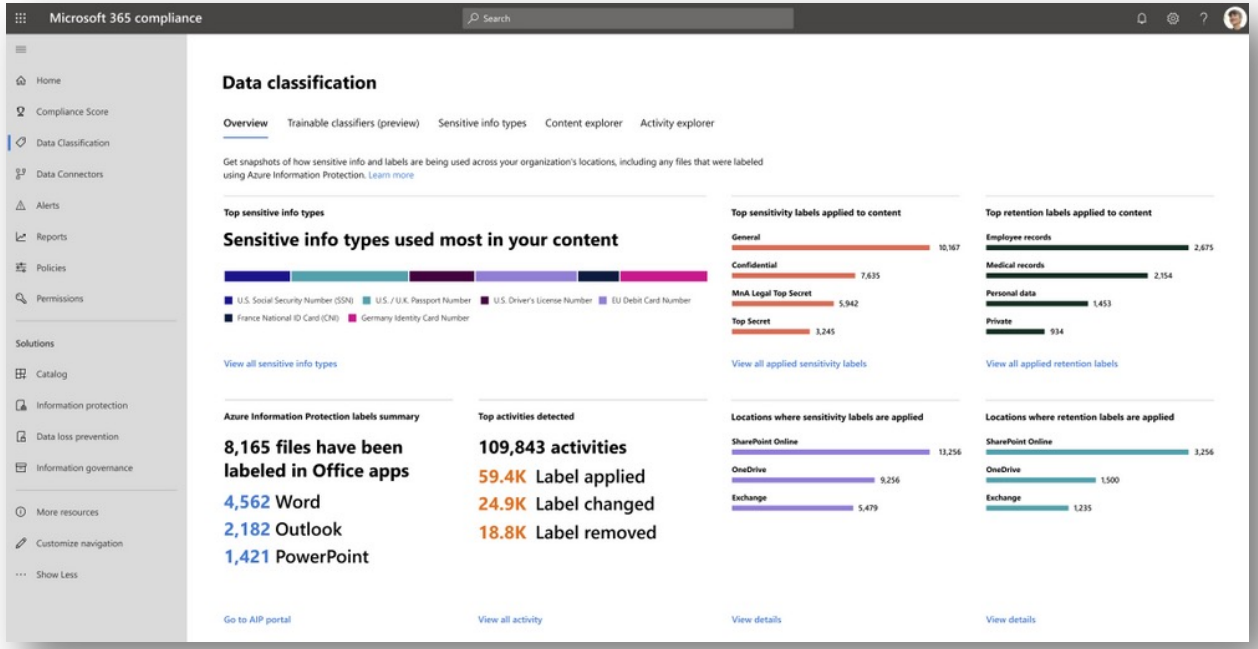
- Management des Daten-Lebenszyklus



Know Your Data

Daten erfassen und klassifizieren

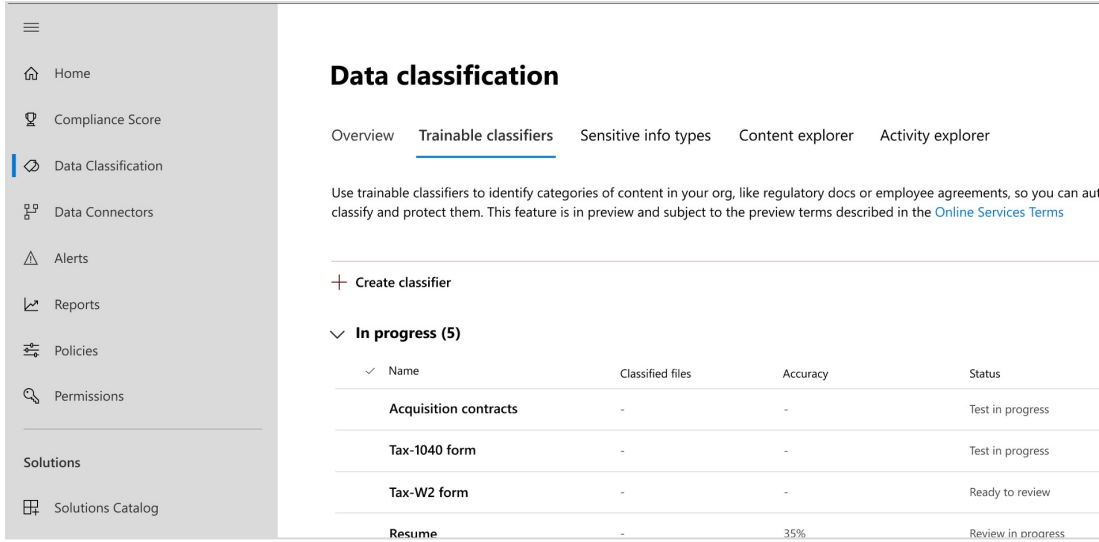
- Typen vertraulicher Informationen
  - Vordefiniert / Benutzerdefiniert
  - Reguläre Ausdrücke, Schlüsselwörter, Wörterbücher
  - Musterübereinstimmungen
  - Näherunsfenster
- Dokument Fingerprinting
  - Vertraulicher Informationstyp basierend auf Standardformular
  - Aktuell nur in Exchange Online
- Exact Data Match (EDM)
  - Genaue Datenwerte, z.B. Kunden- oder Patientendaten



Know Your Data

Daten erfassen und klassifizieren

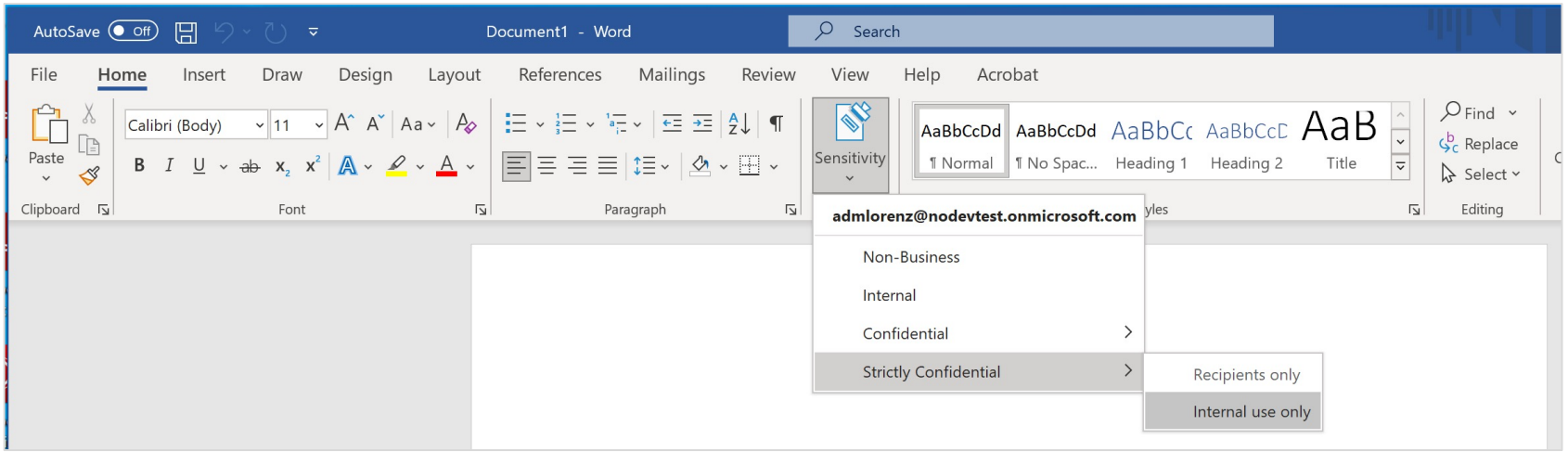
- Trainierbare Klassifizierungsmerkmale
  - Lernt Daten anhand von Beispielen zu erkennen
  - Vordefinierte „ready to use“ Kategorien
  - Benutzerdefinierte Kategorien
- Vertraulichkeitsbezeichnungen
  - Klassifizierungs-Bezeichner (Label)
  - Datenklassifizierung durch Anwender
  - Automatische Klassifizierung
    - Client- oder Service-seitig
    - Basierend auf vertraulichem Informationstyp oder trainierbaren Klassifizierungsmerkmalen



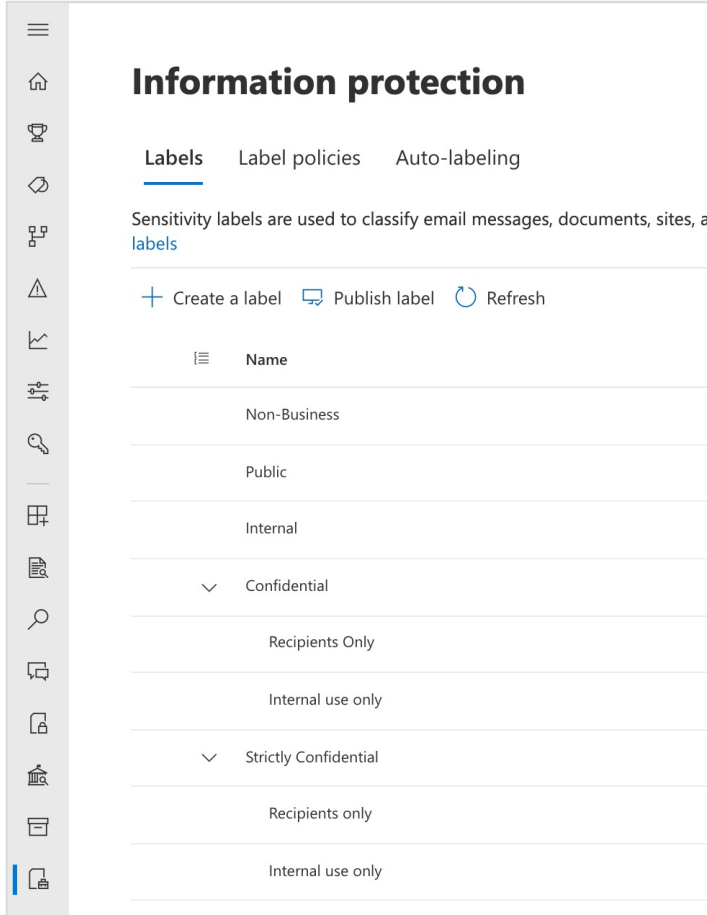
Protect Your Data

Vertraulichkeitsbezeichnungen

- Datenklassifizierung als Abstraktionsschicht
- Maßnahmen basierend auf Bezeichnern
  - Verschlüsselung, Visuelle Markierungen, DLP etc.



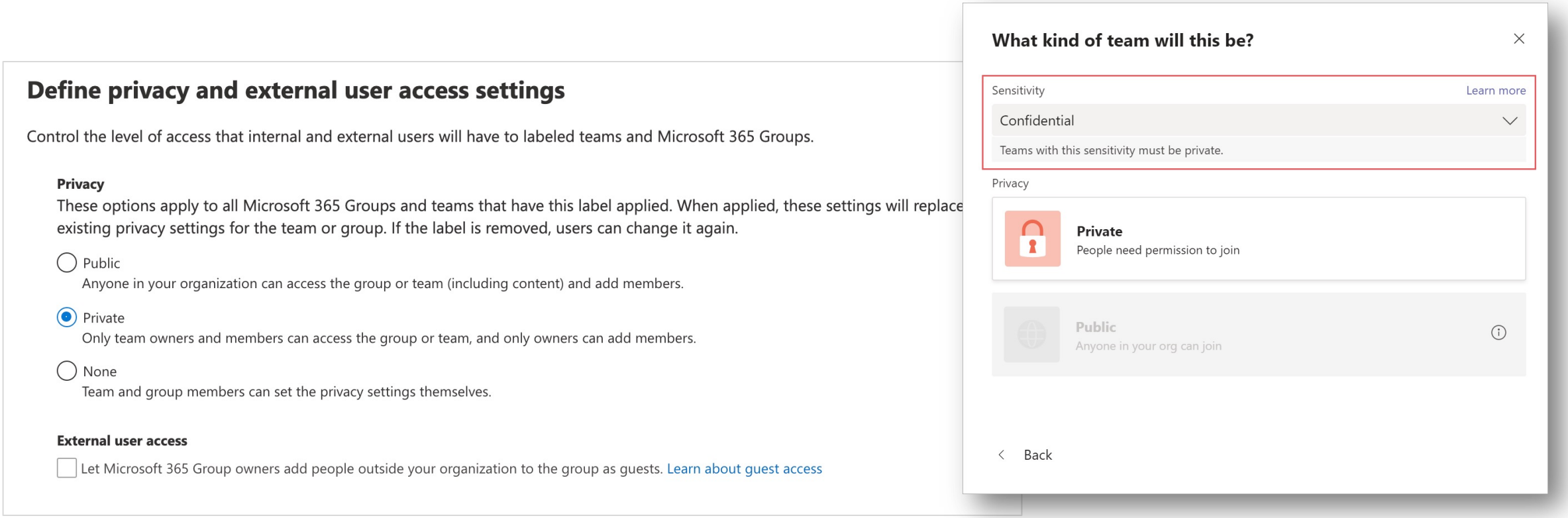




Protect Your Data

Vertraulichkeitsbezeichnungen für Teams, M365 Groups und SharePoint Online Sites

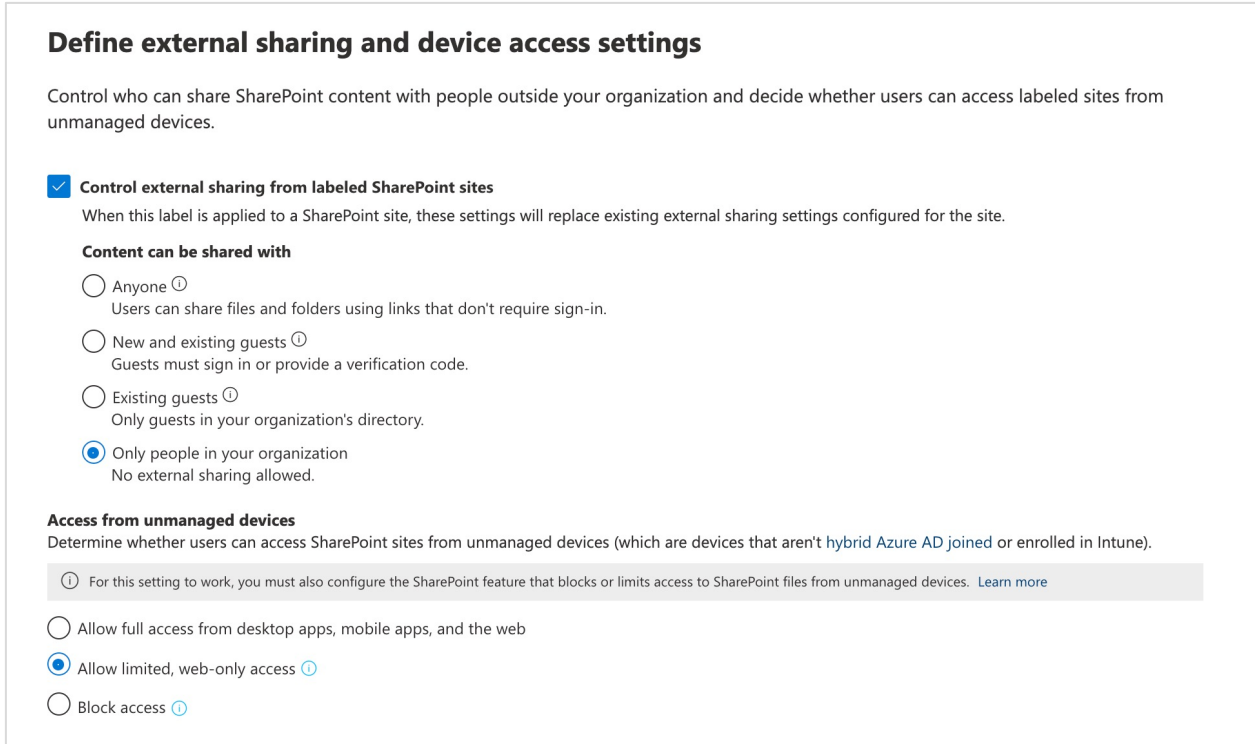
- Verbindliche Einstellungen basierend auf dem Bezeichner



Protect Your Data

Vertraulichkeitsbezeichnungen für Teams, M365 Groups und SharePoint Online Sites

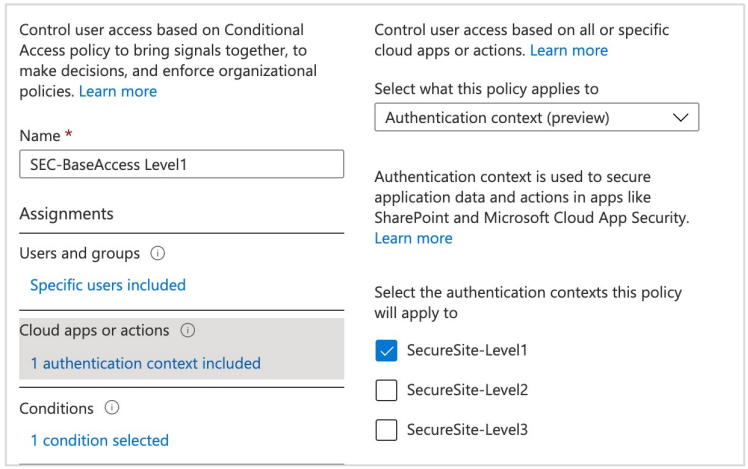
- Einstellungen für Dateifreigaben
- Zugriff mit nicht-verwalteten Geräten
  - Azure AD Conditional Access App-Enforced Restrictions

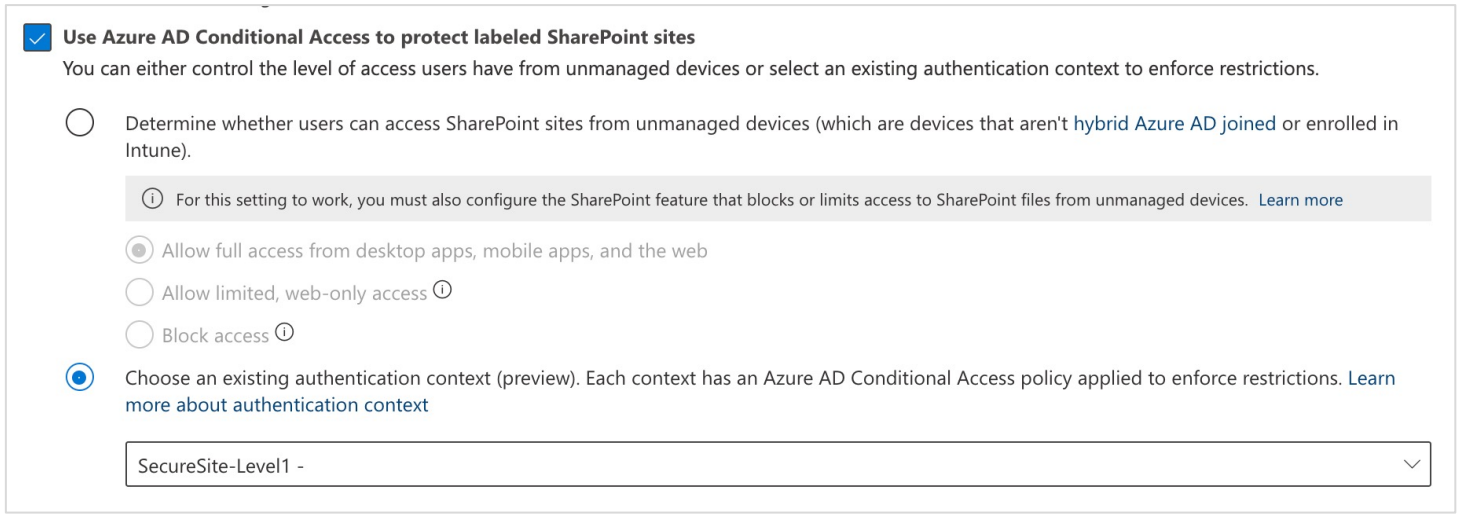


Protect Your Data

Vertraulichkeitsbezeichnungen für Teams, M365 Groups und SharePoint Online Sites

- Integration mit Azure AD Conditional Access Authentication Context
  - Fein-granulare Zugriffssteuerung für SharePoint Sites





Prevent Data Loss

Integration mit Microsoft 365 DLP



Microsoft Teams

Chat Nachrichten
Channel Konversationen



Exchange Online

E-Mail-Versand
E-Mail-Inhalt
Anhänge



SharePoint Online

Indizierte Daten
Dateien aus Teams



OneDrive for Business

Indizierte Daten
Dateien aus Teams-Chats



Office Desktop Apps

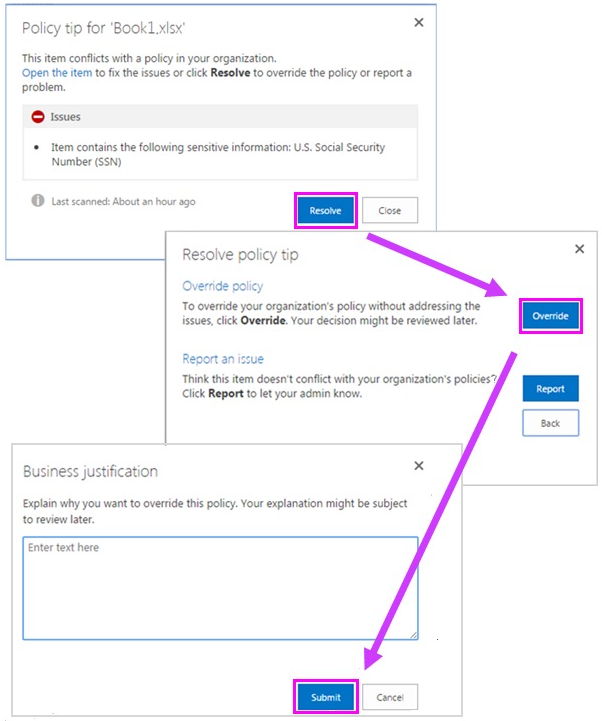
Policy Tipps in Apps
Word
PowerPoint
Excel
Outlook

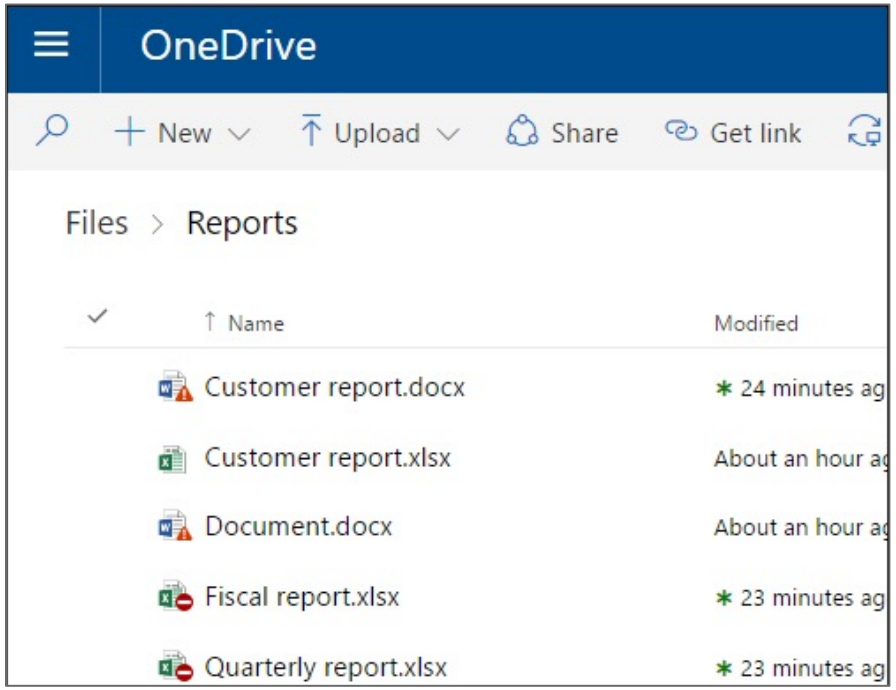
Policy Tipps | Freigaben Blockieren | User Overrides | Hinweis-E-Mails

Prevent Data Loss

Beispiel: SharePoint Freigaben

- DLP-Regeln auf Basis von Bezeichnern
  - Visuelle Hinweise und Richtlinientipps
  - Benutzeraußerkraftsetzen (Override)

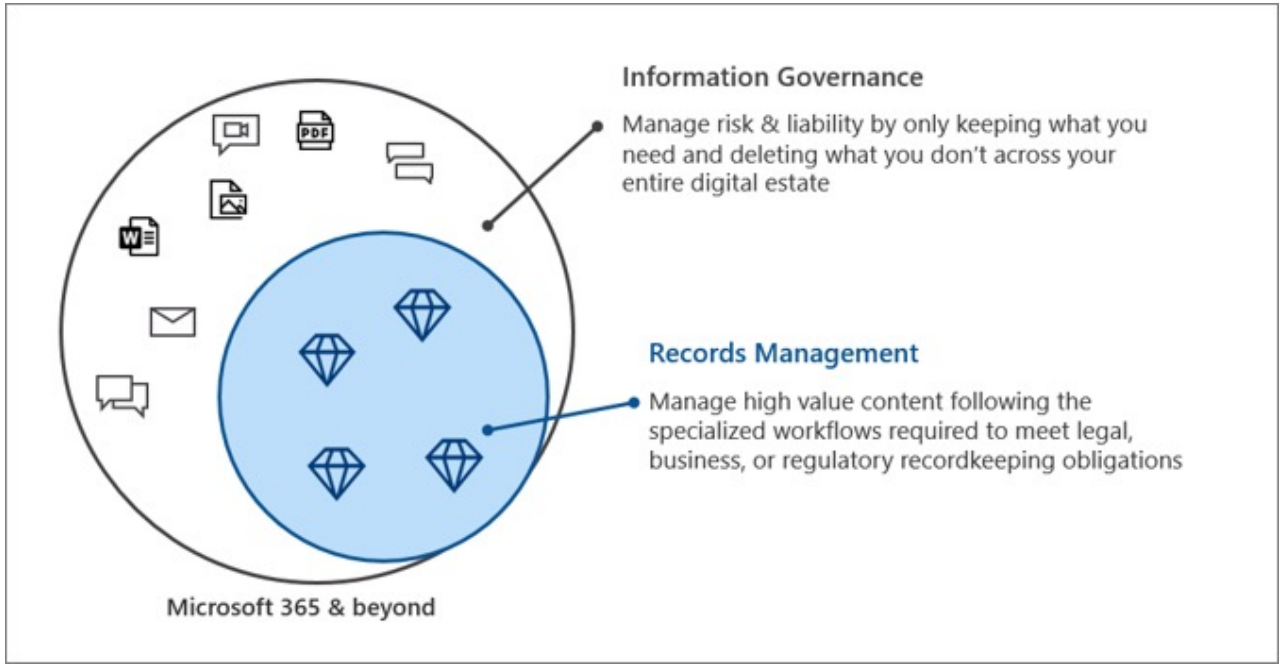




Govern Your Data

Informationsmanagement und Datensatzverwaltung

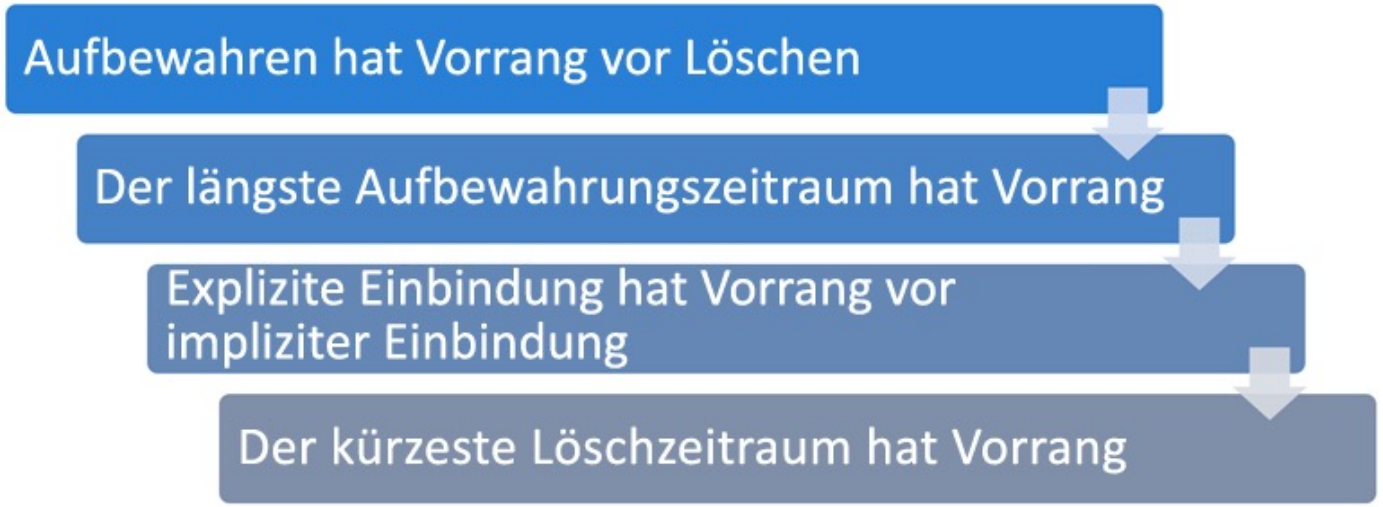
- Aufbewahrungsrichtlinien
- Löschrichtlinien
- Fileplan
- Versionierung
- Disposition



Govern Your Data

Aufbewahren und Löschen von Daten

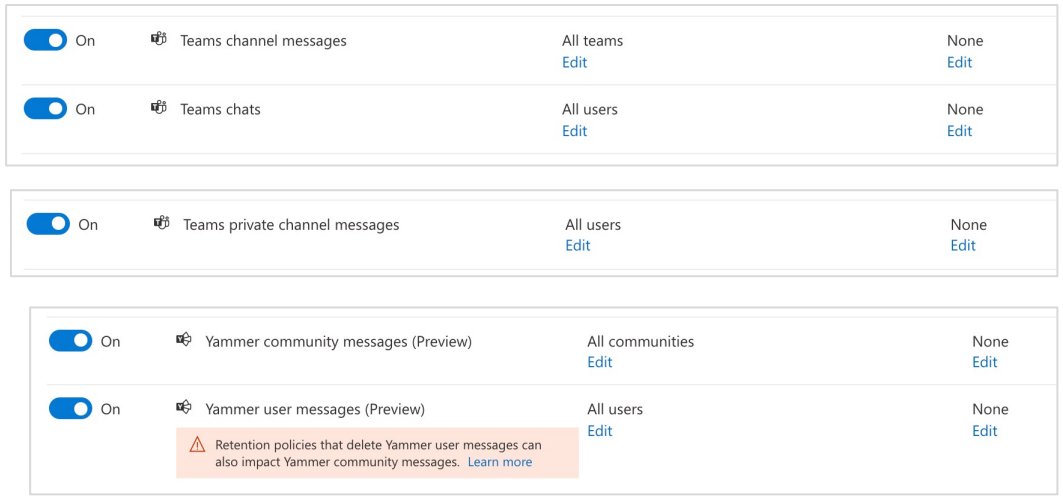
- Inhalte können aufbewahrt, gelöscht oder zuerst aufbewahrt und dann gelöscht werden
  - Ab Erstellung
  - Ab letzter Änderung

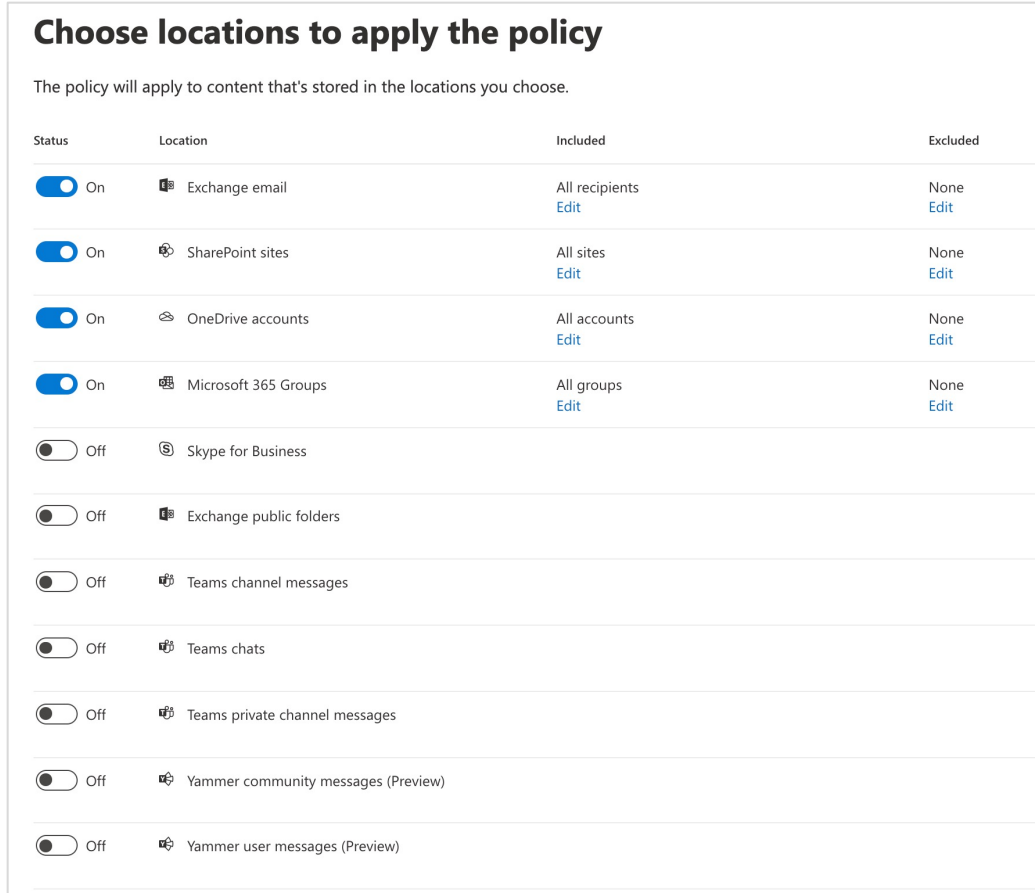


Govern Your Data

Aufbewahren und Löschen von Daten

- Richtlinien für Speicherorte, Benutzer oder Gruppen
  - Separate Richtlinien für:
    - Teams Chats und Channel Nachrichten
    - Teams private Channel Nachrichten
    - Yammer Community und Benutzer Nachrichten (Preview)

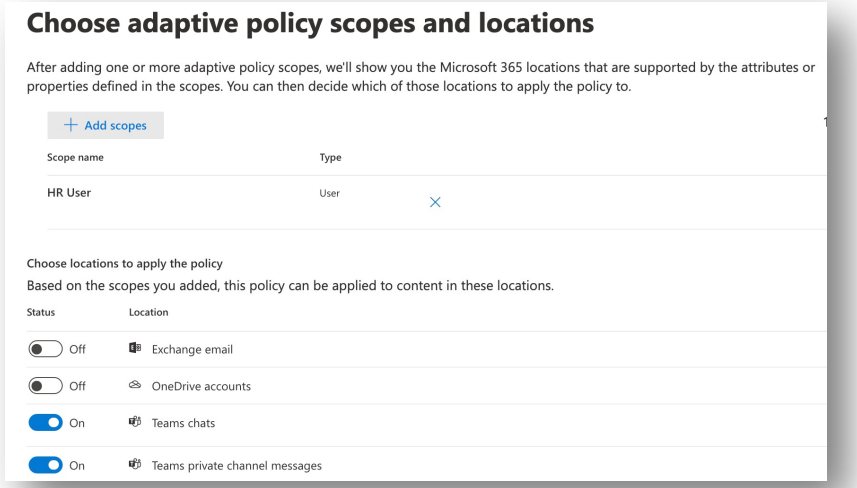


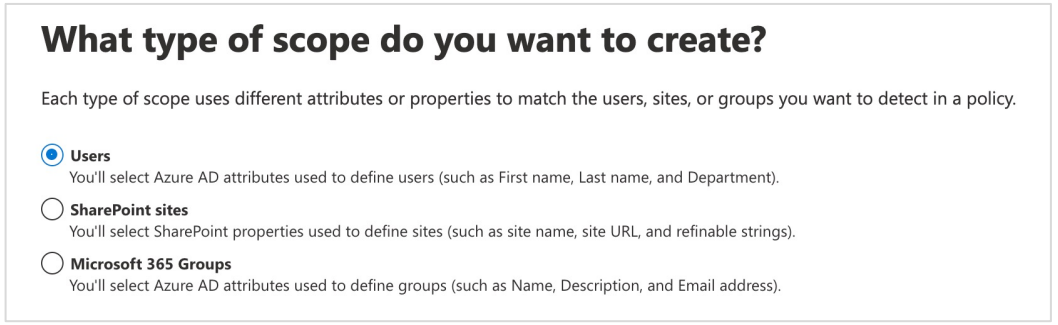


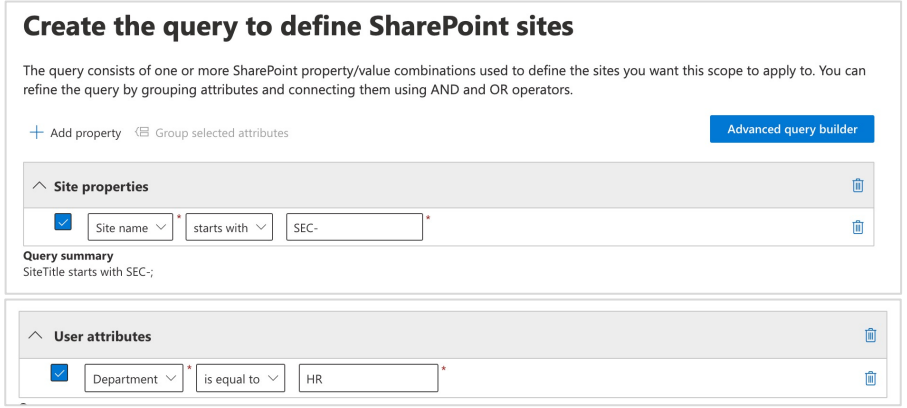
Govern Your Data

Aufbewahren und Löschen von Daten

- Adaptive Scopes (Preview)
  - User, Groups oder Sites
  - Dynamische Zuordnung auf Basis von Attributen
  - Bereich und Datenspeicherort



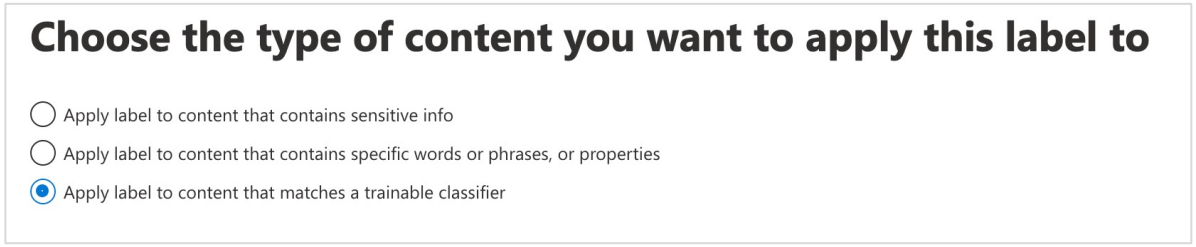


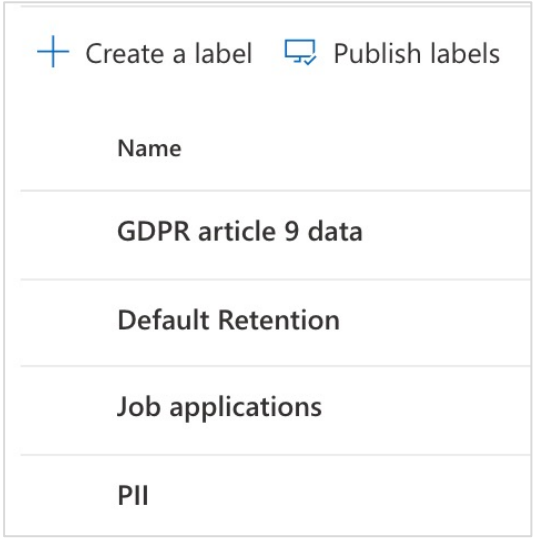


Govern Your Data

Aufbewahren und Löschen von Daten

- Retention Label
  - Direkt auf Daten anwendbar
    - Manuell durch den Anwender
    - Automatisch durch Auto-Labeling Policies
      - Basierend auf vertraulichen Informationstypen, Inhalten (Worte, Ausdrücke, Eigenschaften) oder trainierbaren Klassifizierungsmerkmalen

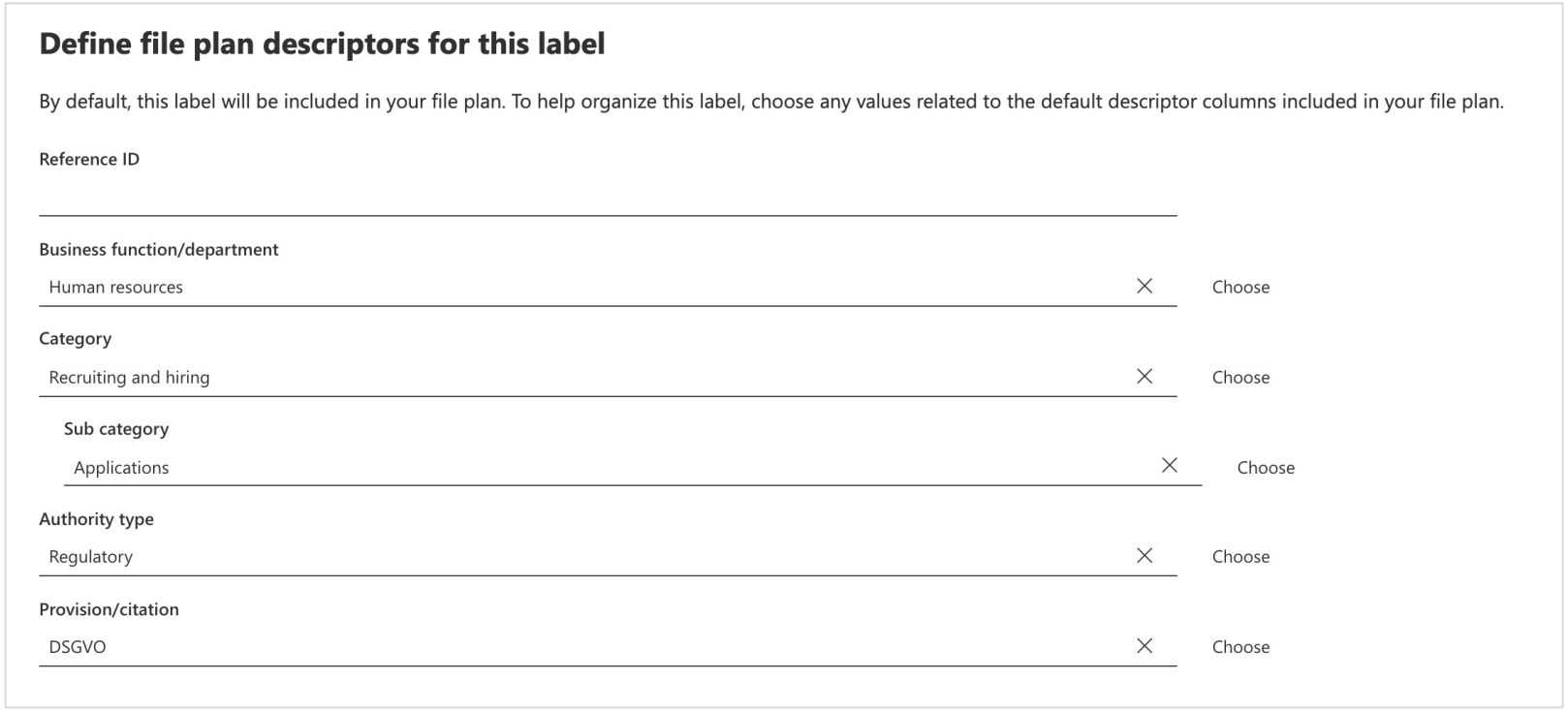




Govern Your Data

File Plan

- Beschreibung von Datensätzen
  - Geschäftsfunktion
  - Kategorie
  - Kontext
  - Quelle

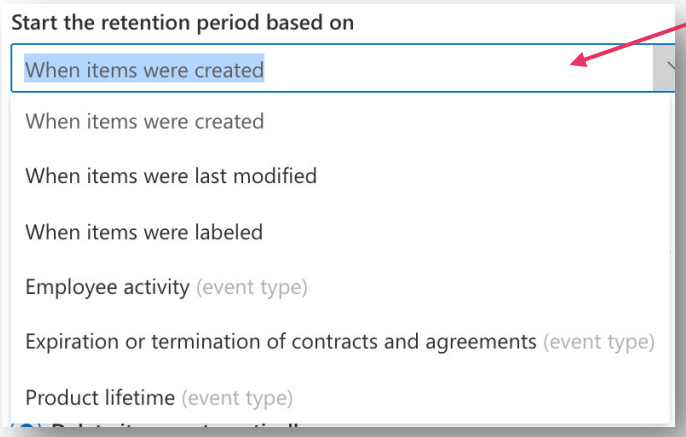


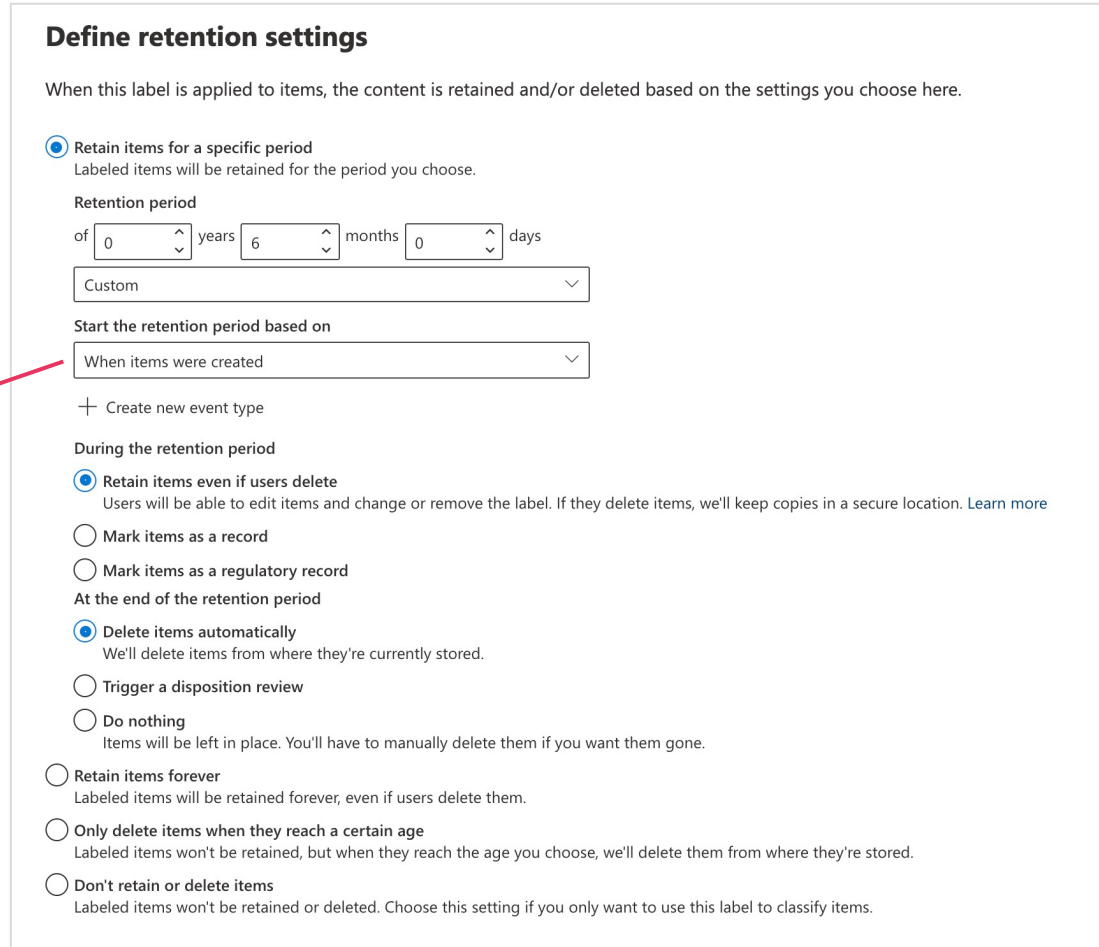
Use file plan to manage retention labels throughout the content lifecycle

Govern Your Data

File Plan

- Definition von Aufbewahrungszeiten und Löschfristen
  - Auslöser: Aufbewahrung ab wann? / Löschen ab wann?
  - Markieren als Datensatz
  - Markieren als regulatorischen Datensatz
  - Disposition Review auslösen

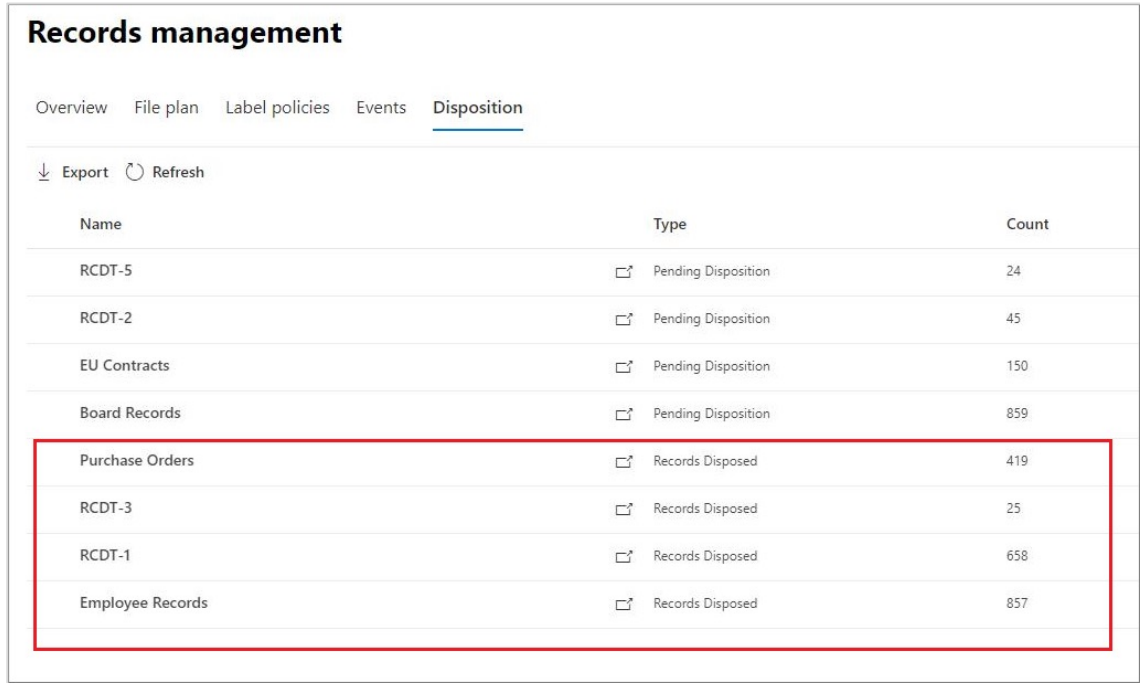




Govern Your Data

Disposition Review

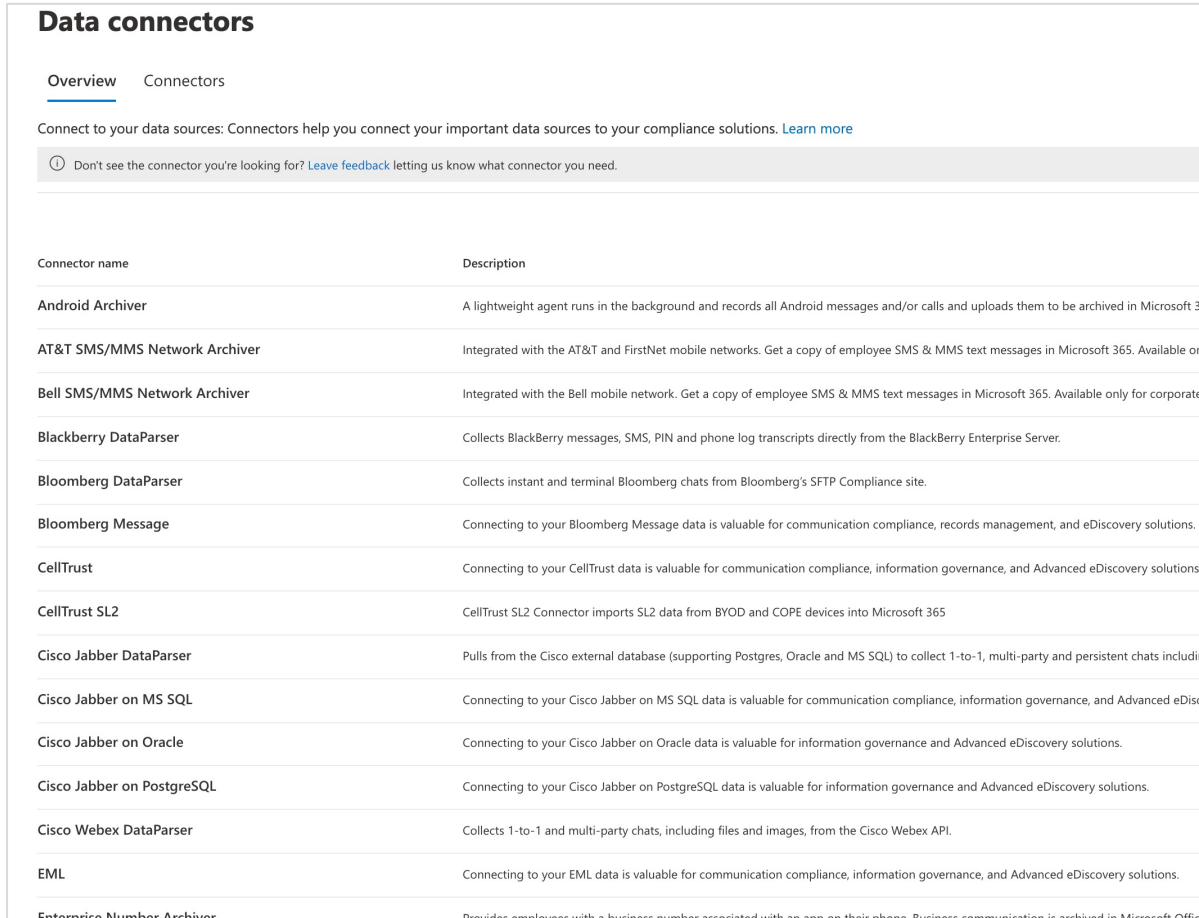
- Überprüfung von Daten, die sich dem Ende ihrer Aufbewahrung nähern
  - Unwiederbringlich löschen
  - Aufbewahrungszeit verlängern
  - Neuen Aufbewahrungsbezeichner anwenden
- Mehrstufige Disposition Reviews



Govern Your Data

Anbindung von Drittanbietern

- Zentrale Compliance-Archivierung
  - Microsoft Daten-Konnektoren
  - Drittanbieter Daten-Konnektoren



Archive third-party data - Microsoft 365 Compliance

Webinar-Reihe „Compliance mit IT“

- Mittwoch, 29.9.2021: Identity Governance & Administration (IGA) im Kontext Compliance (Mitschnitt | Slide Deck)
- Mittwoch, 27.10.2021: *Datenmanagement im Kontext Compliance* (Mitschnitt | Slide Deck)
- Mittwoch, 24.11.2021: *Adressieren von Insider-Risiken* (Anmelden)

Vielen Dank!

Jens Lorenz
Strategic Consultant, CISSP, CSSP, CIPT

mail: jens.lorenz@sits-d.de
fon: +49-170-4516565

LinkedIn: https://de.linkedin.com/in/jenslorenz