silicium consulting

TEAMS SICHERN

SICHERSTELLEN, DASS IHRE DATEN IN MICROSOFT-TEAMS GESCHÜTZT SIND

CONTENTS

CONTENTS

INTRODUCTION

Microsoft Teams ist das Hub für die Teamzusammenarbeit. Was bedeutet das?

Wir können und sollten Teams auf jeden Fall als unseren digitalen Arbeitsplatz oder Desktop nutzen.

Wir können Dateien und Informationen in Teams speichern, Geschäftsanwendungen erstellen, Aufgaben automatisieren, externe Anwendungen/Daten einbetten und für die Kommunikation nutzen. Das sind eine Menge Informationen und Data.

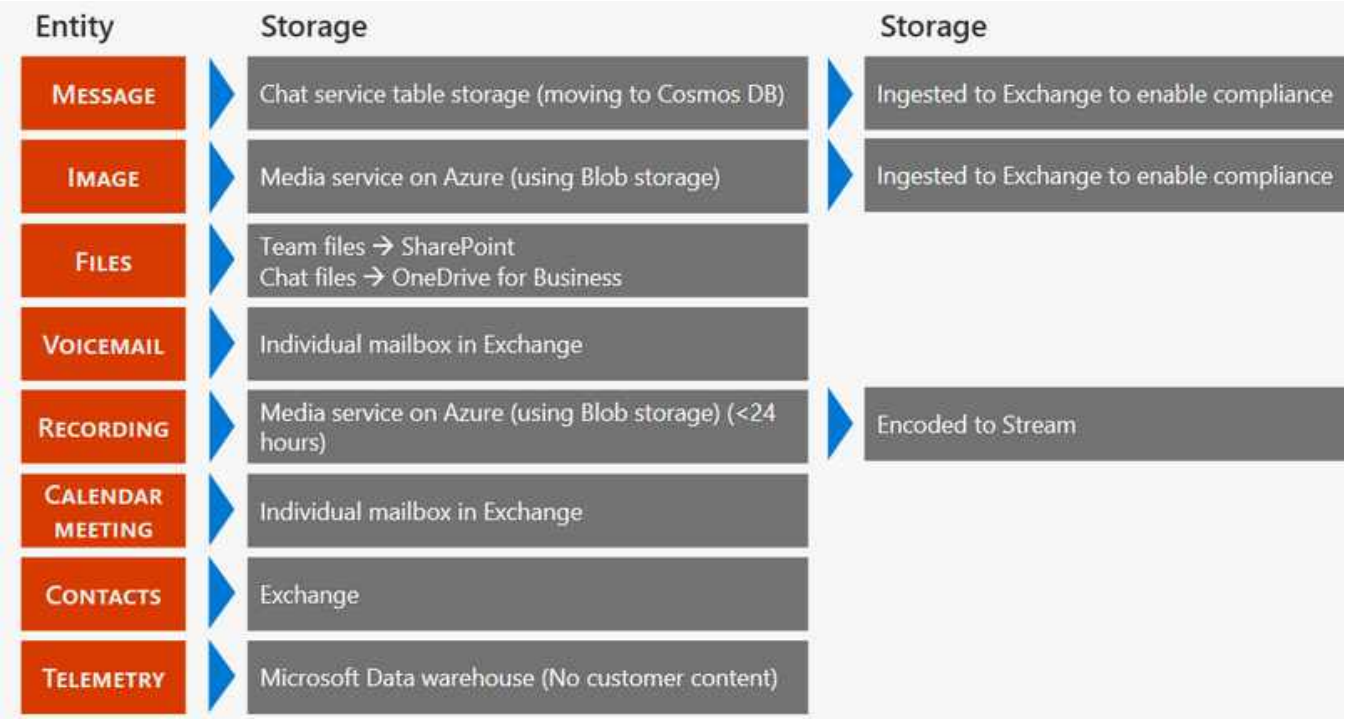
Wir konzentrieren uns oft auf ausgefallene Merkmale und Funktionen (was wir sehen und anfassen können), aber wir müssen auch bedenken, dass alle Daten, die wir speichern, sicher sein müssen. Teams nutzen mehrere Dienste in Microsoft 365, und wir müssen wissen, wo sich unsere Daten befinden, wie wir sie sichern können, wie wir verhindern können, dass Informationen auslaufen, und wie wir unsere Daten sicher gemeinsam nutzen können.

In diesem eBook werden wir uns mit den Sicherheitsfunktionen befassen, die für Teams als Dienst und für verwandte Objekte zur Verfügung stehen. Im Einzelnen werden wir uns mit:

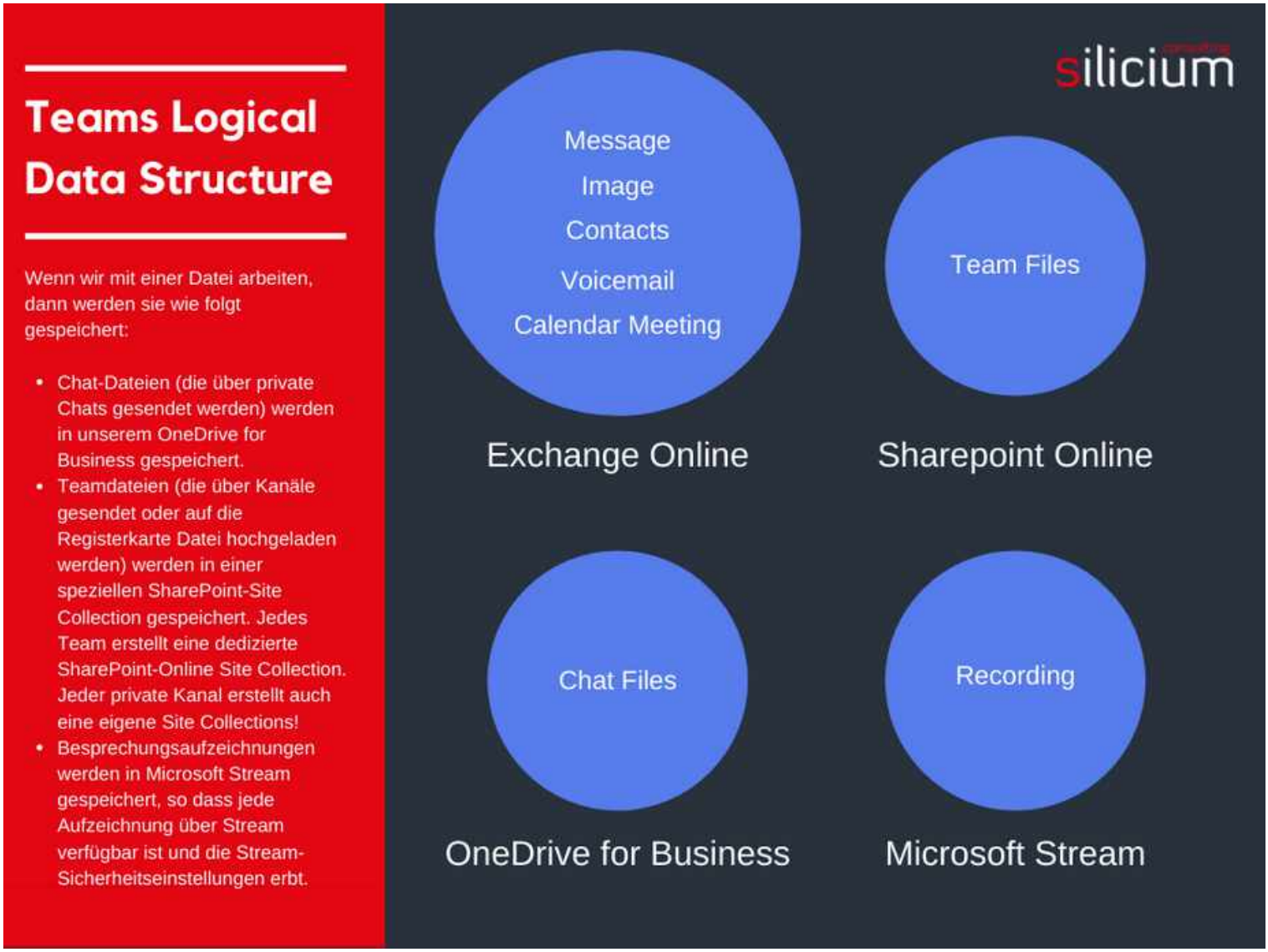
- Wo sich unsere Daten befinden (logisch und physisch), und was bedeutet das?
- Was sind Kennzeichnungen, wann und wie sollen sie verwendet werden?
- Die Löschung ist Teil des Datenlebenszyklus, und wir werfen einen Blick auf diesen Prozess
- Data Loss Preventions - was ist das, und warum brauche ich es?
- Austausch von Informationen mit externen Personen

WO SIND MEINE DATEN?

Es gibt keinen einzigen Ort, an dem Teams ihre Daten speichern. Tatsächlich gibt es bei Microsoft 365 und Azure viele verschiedene Dienste, bei denen Daten gespeichert werden. Dieses Wissen ist wichtig, um die Mechanismen zu verstehen und unsere Informationen richtig zu sichern.



Dieses Diagramm beschreibt, wo jeder Teil der Daten gespeichert wird. Es mag kompliziert aussehen, aber wir können es leicht auf eine logischere Weise zeigen.



PHYSIKALISCHER DATENSTANDORT

Logische Datenorte sind nur ein Teil der Gleichung. Der physische Speicherort jeder Datei ist auch deshalb wichtig, weil wir in einer Welt voller Vorschriften und Gesetze leben. Jedes Land kann Vorschriften und Verpflichtungen für die Datenspeicherung festlegen. Es gibt auch globale Vorschriften (z.B. EU). Aus diesem Grund stellt Microsoft Informationen zum Datenaufenthalt für die wichtigsten Dienste in Microsoft 365 zur Verfügung.

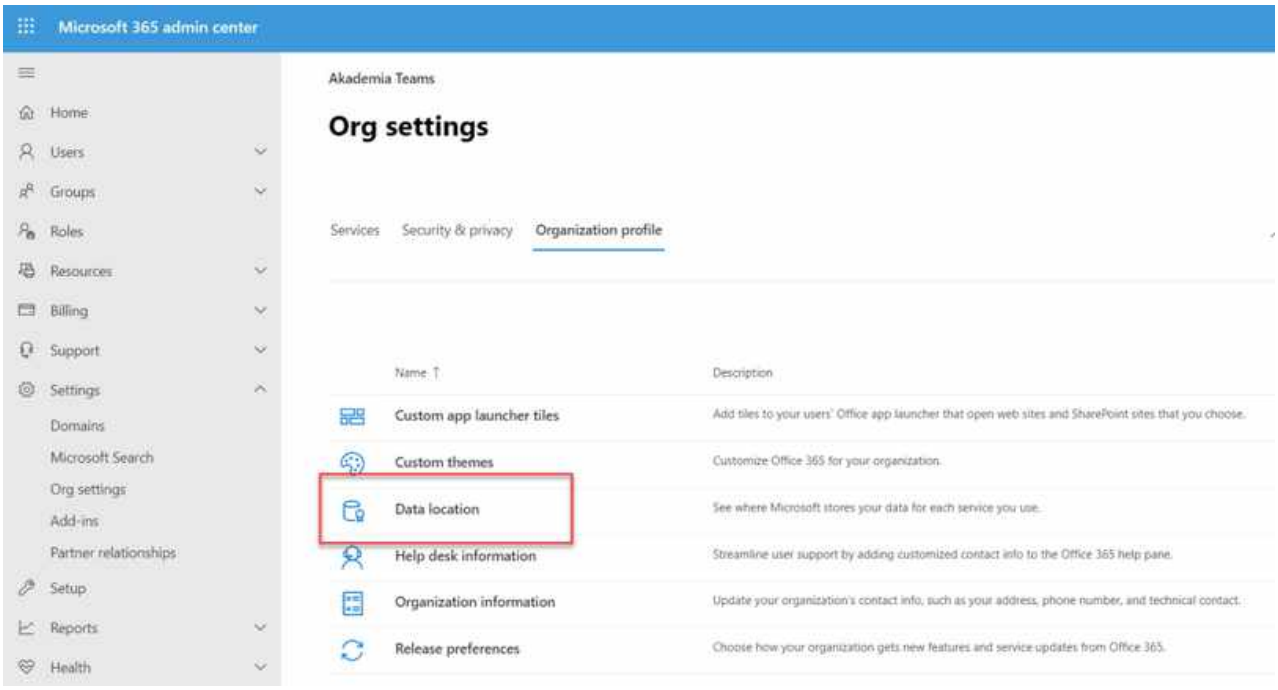
Microsoft investiert viel Aufwand, um mehr Rechenzentren in der Nähe Ihres geografischen Standorts bereitzustellen. Für aktuelle Daten sollten Sie diese Seite für Updates besuchen:

https://docs.microsoft.com/de-de/microsoftteams/location-of-data-in-teams

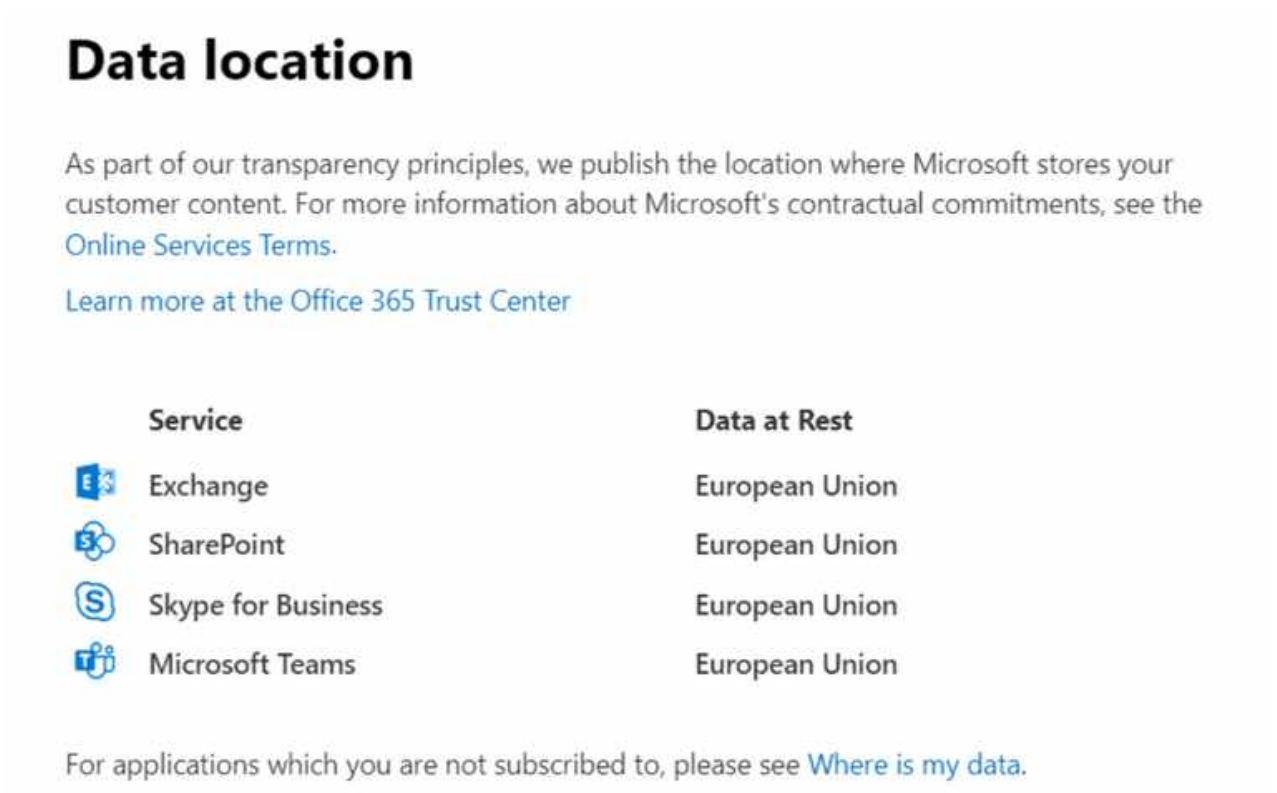
Sie können auch manuell überprüfen, wo sich Ihre Tenant Daten befinden. Dazu müssen Sie über globale Administratorrechte auf Microsoft 365 verfügen.

Quick Steps:

1. Gehen Sie zum Microsoft 365 Admin Center (https://portal.office.com/adminportal/home)
2. Auf **Einstellungen** klicken im linken Menü
3. Gehen Sie zu den Abschnitten des Organisationsprofils und wählen Sie die Option Datenspeicherort.



4. Sie erhalten detaillierte Informationen über jede Dienst. In diesem Beispiel befinden sich alle Daten (für Exchange Online, SharePoint Online, Skype für Unternehmen und Microsoft Teams) in der Europäischen Union.



Vertraulichkeitsbezeichnungen und Klassifikations Labels

Es gibt zwei Arten von Labels:

- Vertraulichkeitsbezeichnungen
- Klassifikations Labels

Klassifikations Labels sind Labels, die mit einem Teil der Daten verbunden sind (z.B. List Item, Dokument, Team usw.). Sie können solche Labels erstellen und sie als Metadaten verwenden.

Vertraulichkeitsbezeichnungen sind Einstellungen, die es Ihnen ermöglichen, Richtlinien und Regeln auf der Grundlage dieser Labels automatisch zuzuweisen. Vertraulichkeitsbezeichnungen sind nicht auf Teams beschränkt - wir können sie in SharePoint-Websites und Microsoft 365-Gruppen verwenden.

Vertraulichkeitsbezeichnungen in PowerShell aktivieren

Um Vertraulichkeitsbezeichnungen zu ermöglichen, müssen wir die folgenden Schritte durchlaufen:

1.Öffnen Sie ein Windows PowerShell-Fenster auf Ihrem Computer. Sie können es ohne erhöhte Rechte öffnen

2. Führen Sie die folgenden Befehle aus, um die Ausführung der Cmdlets vorzubereiten.

```
Import-Module AzureADPreview
Connect-AzureAD
```

3. Geben Sie auf der Seite Bei Ihrem Konto anmelden Ihr Administratorkonto und das zugehörige Kennwort ein, um eine Verbindung mit dem Dienst herzustellen, und wählen Sie Anmelden aus.

4. Rufen Sie die aktuellen Gruppeneinstellungen für die Azure AD-Organisation ab.

```
$Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | where -Property DisplayName -Value "Group.Unified" -EQ).id
```

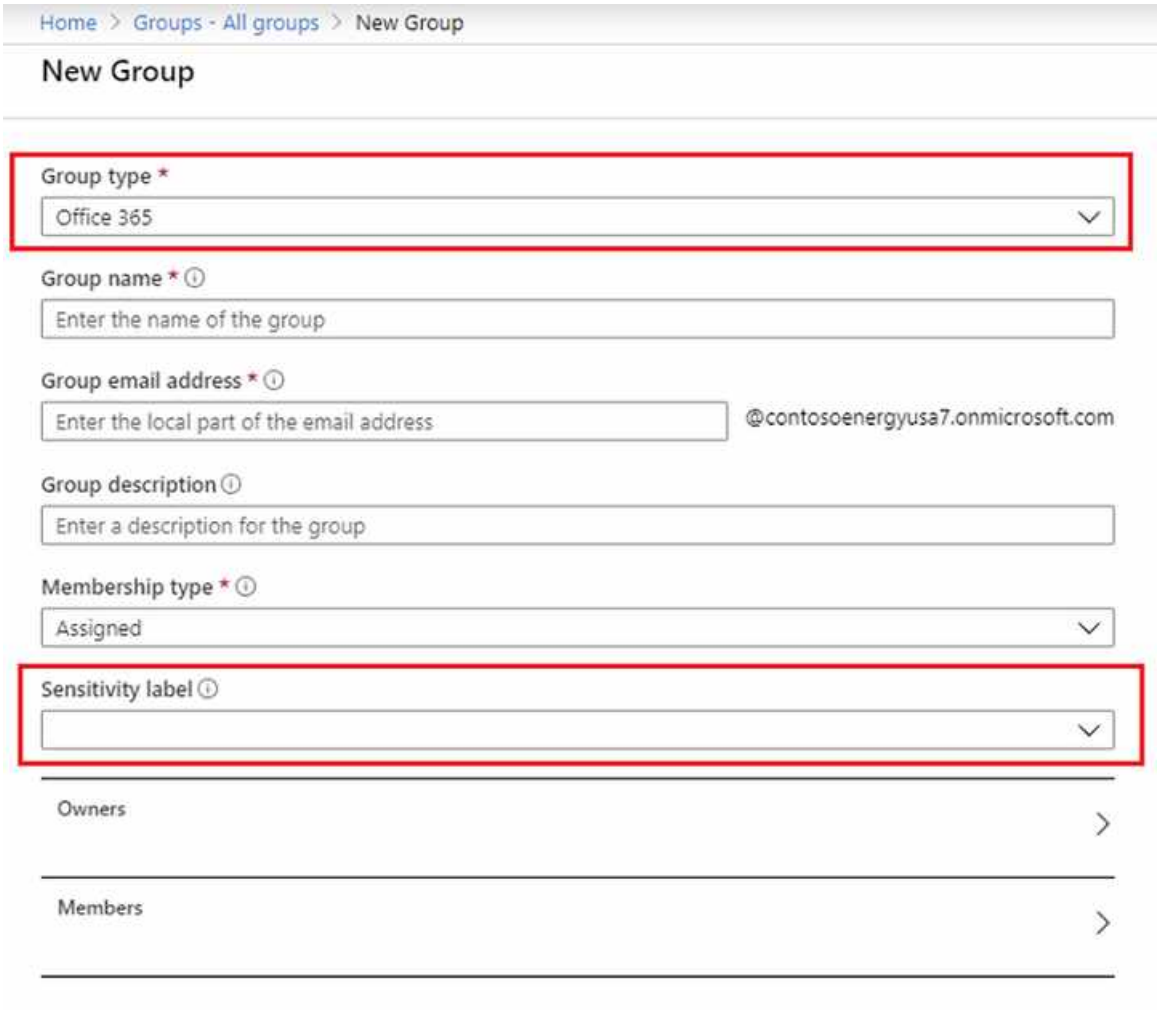
5. Labels aktivieren

```
$Setting["EnableMIPLabels"] = "True"
```

6. Einstellungen speichern

```
Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
```

Um die Konfiguration schnell zu überprüfen, können Sie zum Azure AD Admin Center navigieren, **Groups** wählen, und dann **Neue Gruppe**. Ändern Sie **Gruppentyp** in **Office 365**, und nun sollten Sie in der Lage sein, **Vertraulichkeitsbezeichnungen** auszuwählen.



Problembehandlung

Obwohl Sie alle oben genannten Schritte befolgt haben, kann es sein dass Sie immer noch nicht die Einstellungen in Azure Active Directory sehen. Möglicherweise müssen Sie das Compliance Center (https://compliance.microsoft.com/) besuchen und sicherstellen, dass es initialisiert ist und die ersten Überprüfungen in Ihrer Umgebung durchführt.

Sie werden auch sicher sein wollen, dass die folgenden Anforderungen ebenfalls erfüllt sind:

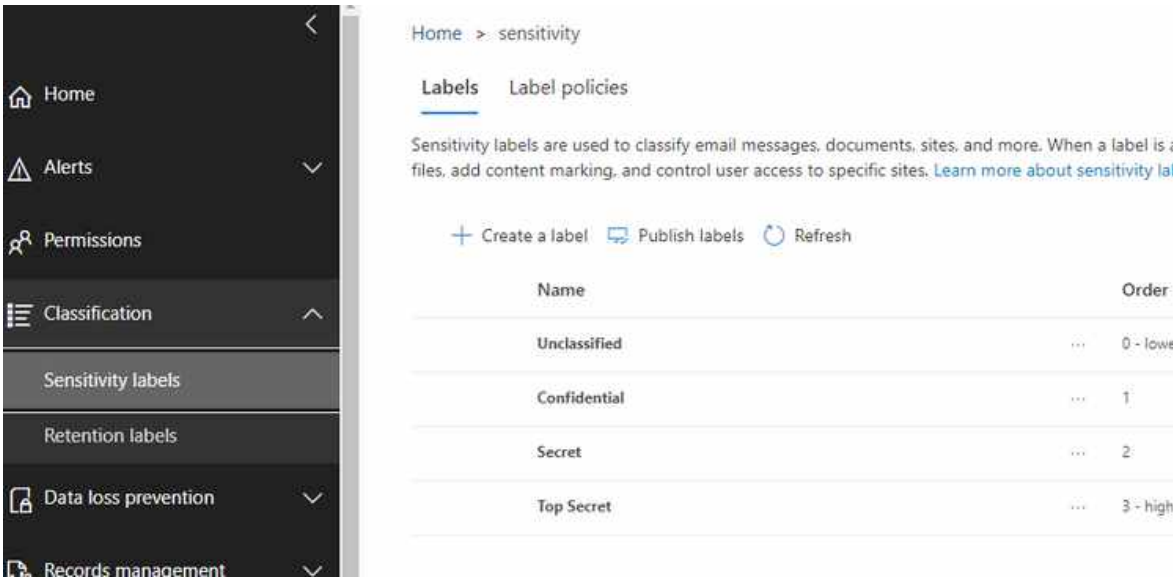
- Das Feature ist aktiviert, „EnableMIPLabels“ ist in PowerShell auf „True“ festgelegt.Die Gruppe ist eine Office 365-Gruppe.
- Der aktuell angemeldete Benutzer verfügt über ausreichende Berechtigungen, um Bezeichnungen zuzuweisen. Der Benutzer muss entweder ein globaler Administrator, ein Gruppenadministrator oder der Gruppenbesitzer sein.

Vertraulichkeitsbezeichnungen erstellen

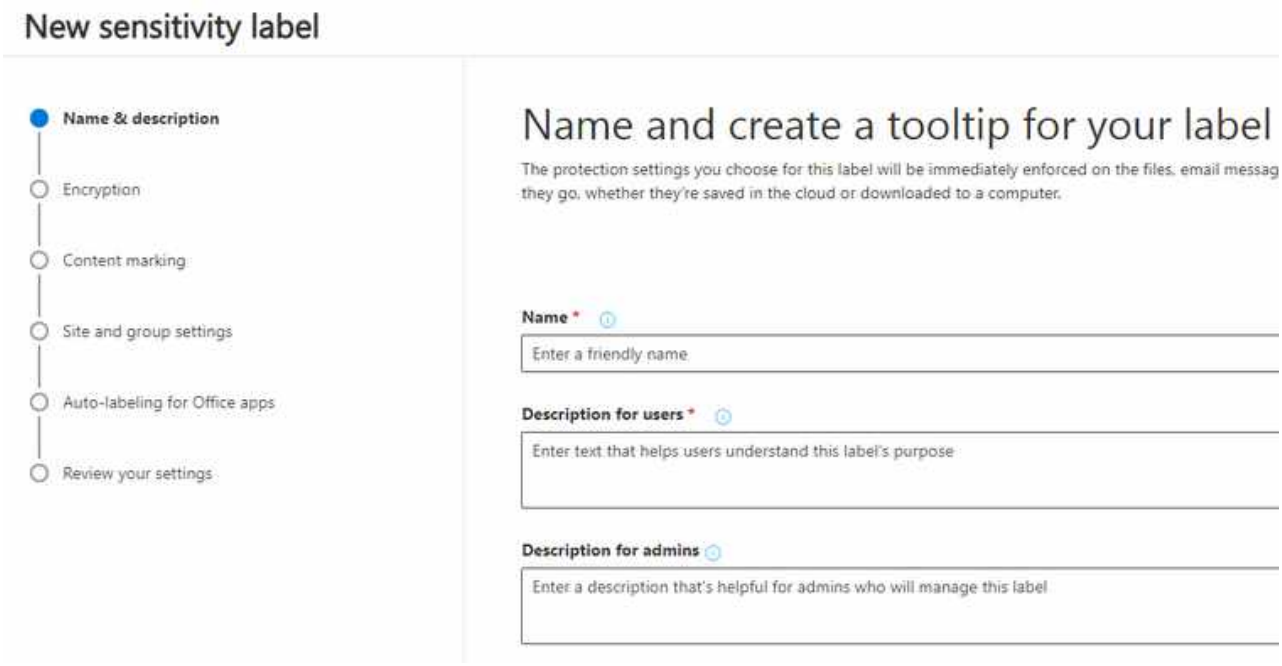
Wenn Sie die obigen Schritte abgeschlossen haben, können Sie zum Microsoft 365 Security and Compliance Center (https://protection.office.com/) gehen und Ihr erstes Label erstellen.

Erste Schritte:

1. Zu Office 365 Security & Compliance Admin Center (https://protection.office.com/) navigieren.

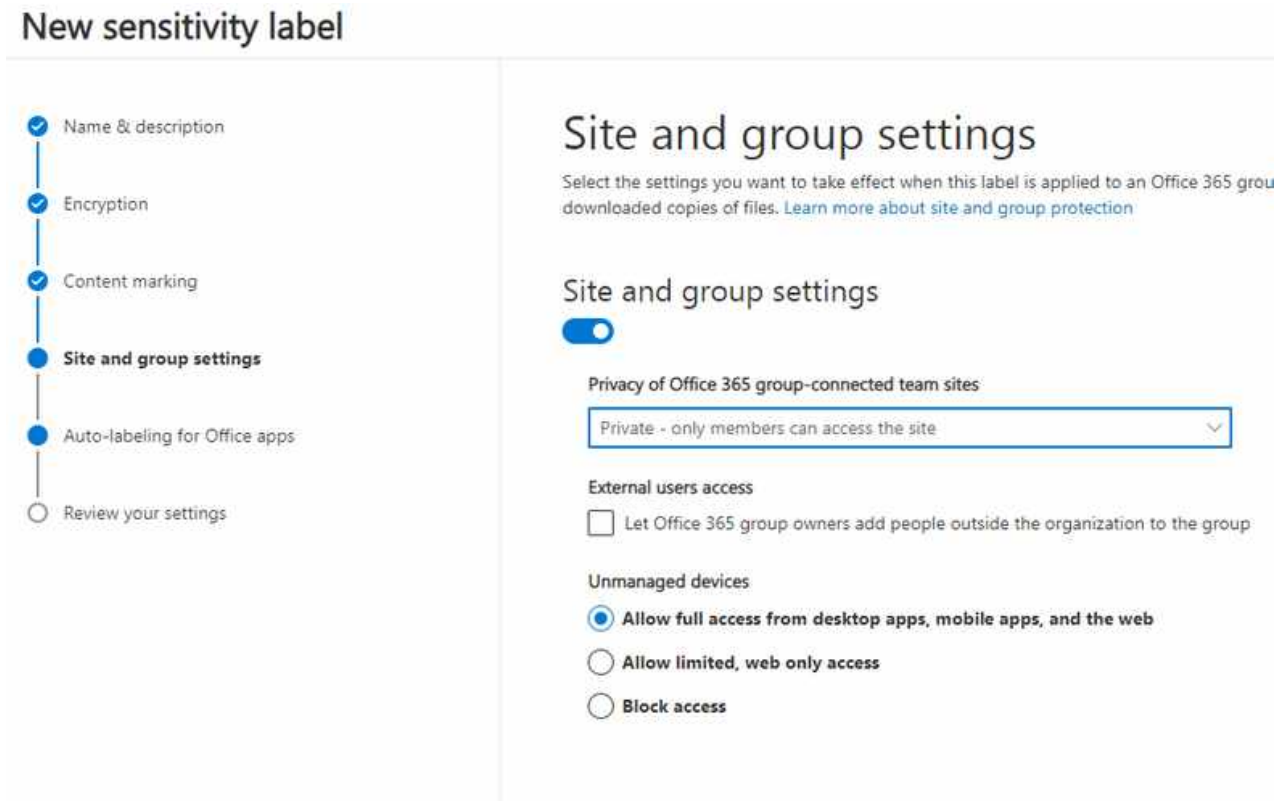


2. Klicken Sie auf Create a label und ein neues Formular wird angezeigt.



3. Füllen Sie die erforderlichen Felder auf jeder Seite aus

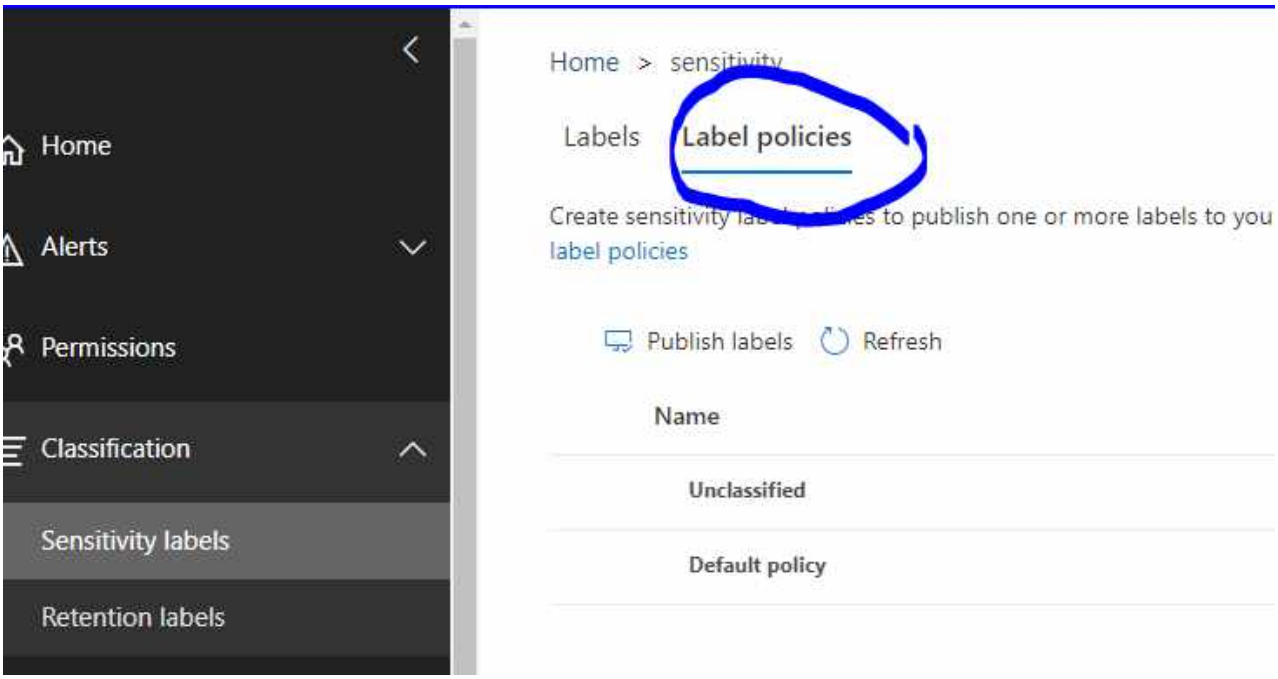
4. Auf der Seite Site- und Gruppeneinstellungen können Sie Sicherheitsoptionen für die Microsoft 365-Gruppe oder SharePoint-Website auswählen



5. Überprüfen Sie auf der letzten Seite die Informationen und erstellen Sie ein Etikett

Jetzt können wir eine neue Label-Richtlinie erstellen und veröffentlichen.

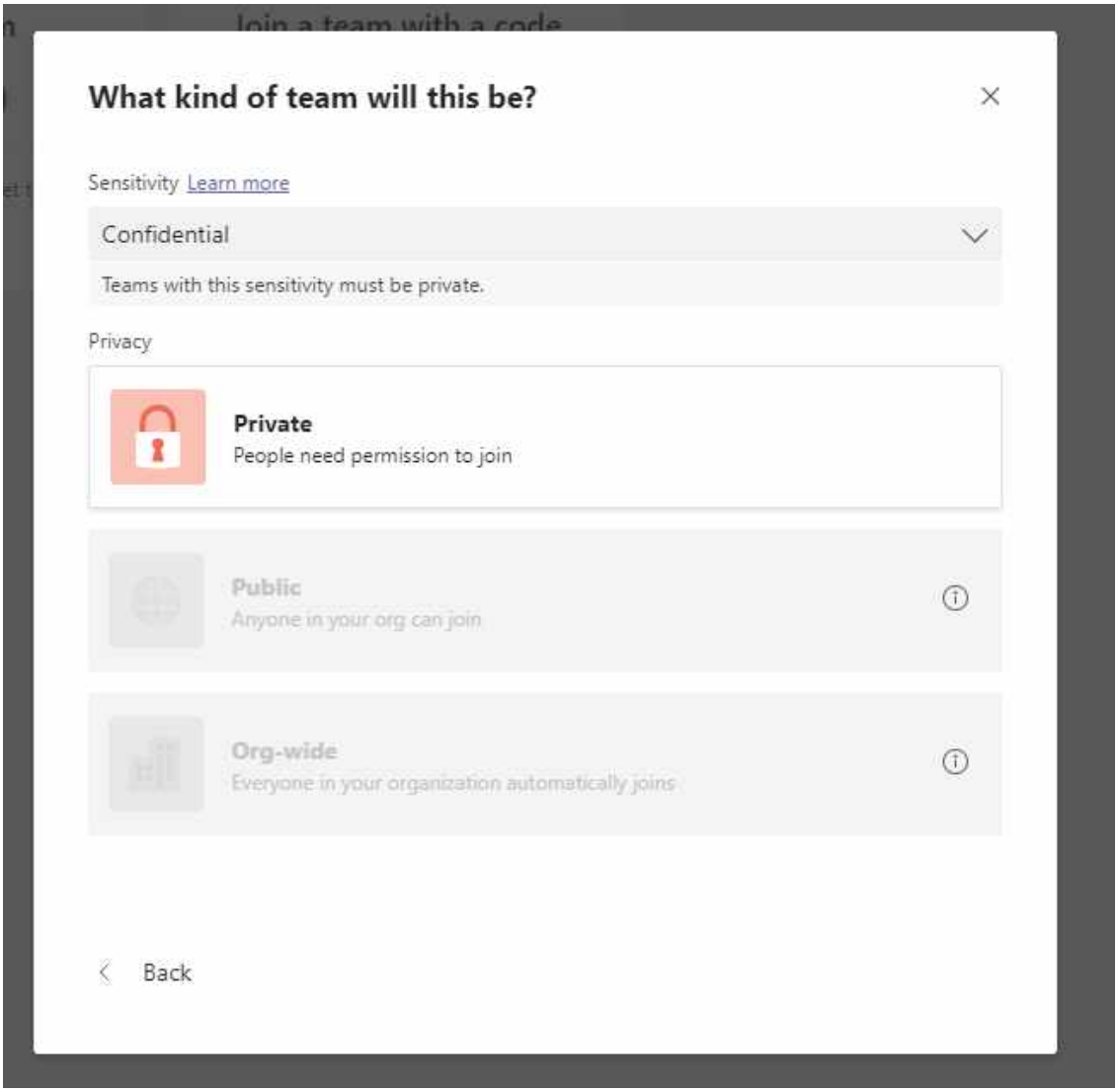
1. Gehen Sie zur Registerkarte Label-Richtlinien und klicken Sie auf Labels veröffentlichen



2. Zuerst müssen wir unser neues Label auswählen,und **veröffentlichen**.

Und jetzt unser Label ist Ready-to-go! Um zu prüfen, wie es funktioniert, können wir versuchen, ein neues Team zu bilden.

5. Überprüfen Sie auf der letzten Seite die Informationen und erstellen Sie ein Etikett



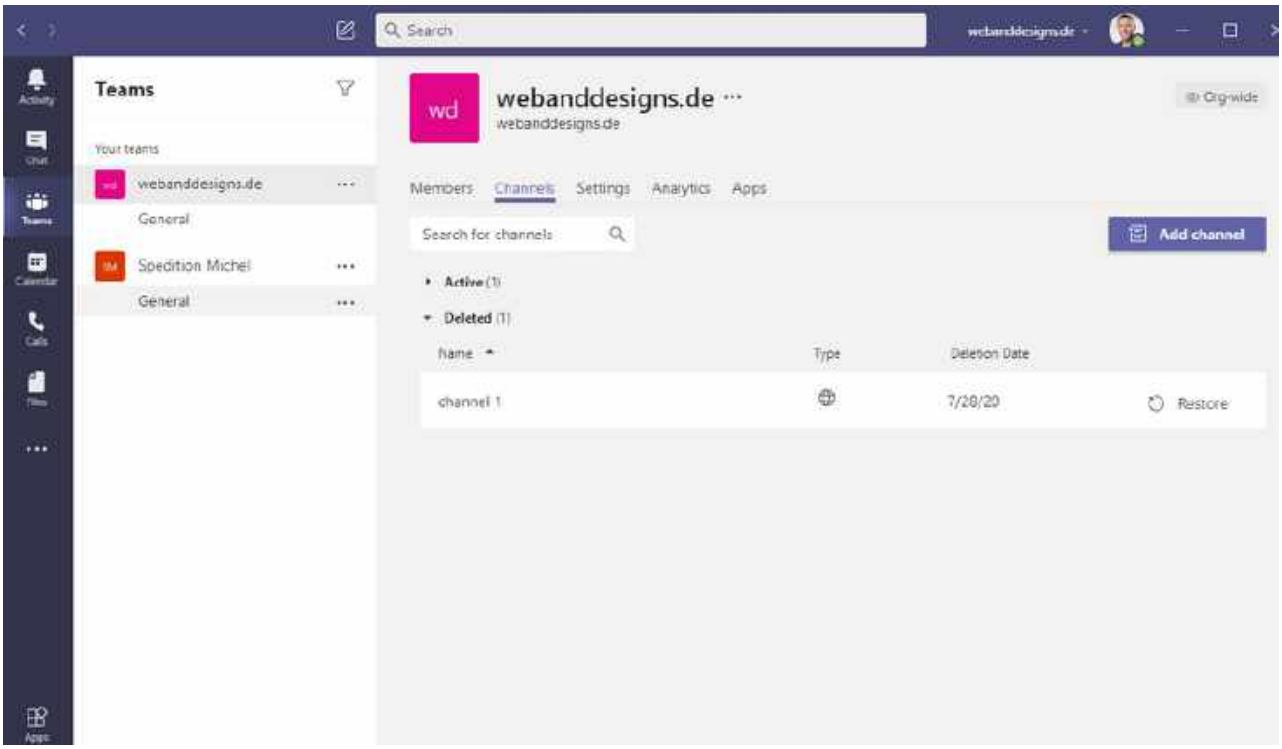
Wie Sie sehen, ist die Dropdown-Liste "Sesitivity" verfügbar, und wir können nur private Teams auswählen. Das liegt an unseren Label Einstellungen.

Löschen und Wiederherstellen von Teams Objekten

Jedes Objekt in Teams kann gelöscht werden - Datei, Element, Nachrichten, Kanal, Team usw. (wir brauchen die richtigen Berechtigungen und die richtige Konfiguration, um Objekte löschen zu können). Wenn wir ein Objekt versehentlich löschen oder wenn wir dieses Objekt wiederherstellen müssen, gibt es mehrere Möglichkeiten.

Gelöschten Kanal wiederherstellen

Um einen Kanal wiederherzustellen, müssen wir zum Abschnitt Team verwalten gehen, Kanäle auswählen und dann im Bereich Gelöscht den entfernten Kanal auswählen. Dann können wir einfach auf die Schaltfläche Wiederherstellen klicken (Dateien und Konversationen werden wiederhergestellt).



Gelöschtes Team wiederherstellen

Wir können das entfernte Team mit PowerShell oder über die Azure AD-Portalseite wiederherstellen.

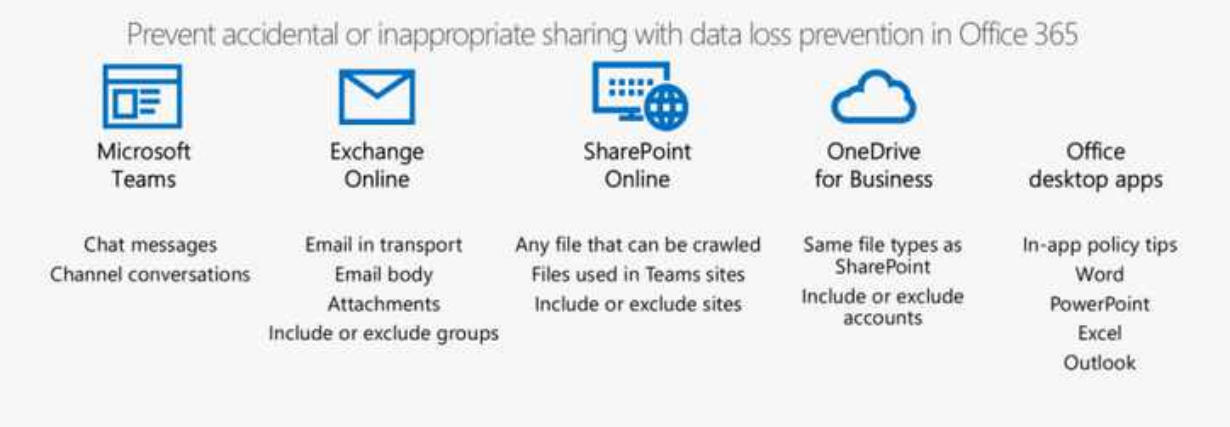
Gehen Sie zu Azure AD Portal, wählen Sie Gruppen und dann Gelöschte Gruppen. Sie erhalten eine Liste aller gelöschten Microsoft 365 Gruppen innerhalb der letzten 30 Tage. Um eine Gruppe wiederherzustellen, wählen Sie einfach die Gruppe aus, die wiederhergestellt werden soll, und klicken Sie auf Gruppe wiederherstellen. Gelöschte Gruppen, die nicht wiederhergestellt werden, werden nach 30 Tagen dauerhaft entfernt!

Data Loss Prevention

Informations- oder Datenverlust sind sehr häufig und können einer Organisation erheblichen Schaden zufügen. Wir können Datenverlust in zwei Kategorien einteilen - absichtliche Handlungen und versehentliche Handlungen. Bei absichtlichen Handlungen müssen wir auf vielen verschiedenen Ebenen absichern, dies liegt außerhalb des Rahmens dieses eBook.

Unbeabsichtigte Aktionen können durch mangelnde Verfahrenskenntnisse, fehlende Informationsrichtlinien, schlechte Informationsgewohnheiten usw. verursacht werden. In vielen Fällen ist es sehr einfach - die Menschen wissen nicht, dass bestimmte Informationen vertraulich sind, und sie senden sie über offene Kanäle oder an externe Personen.

Um diese Art von Datenverlust zu verhindern, können wir den Data Loss Prevention-Mechanismus innerhalb von Microsoft 365 verwenden.



In Teams kann DLP uns unterstützen:

Sensibler Informationen in Nachrichten zu schützen

Angenommen, ein Mitarbeiter versucht, sensible oder vertrauliche Informationen über den Chat mit einem externen Benutzer in Teams zu senden. Wenn wir eine DLP-Richtlinie einrichten, können wir Chats mit der externen Welt überwachen und die Kommunikation blockieren, die bestimmte Informationen enthält (z.B. Versicherungsnummern, Kreditkartennummern, firmenspezifische Daten).

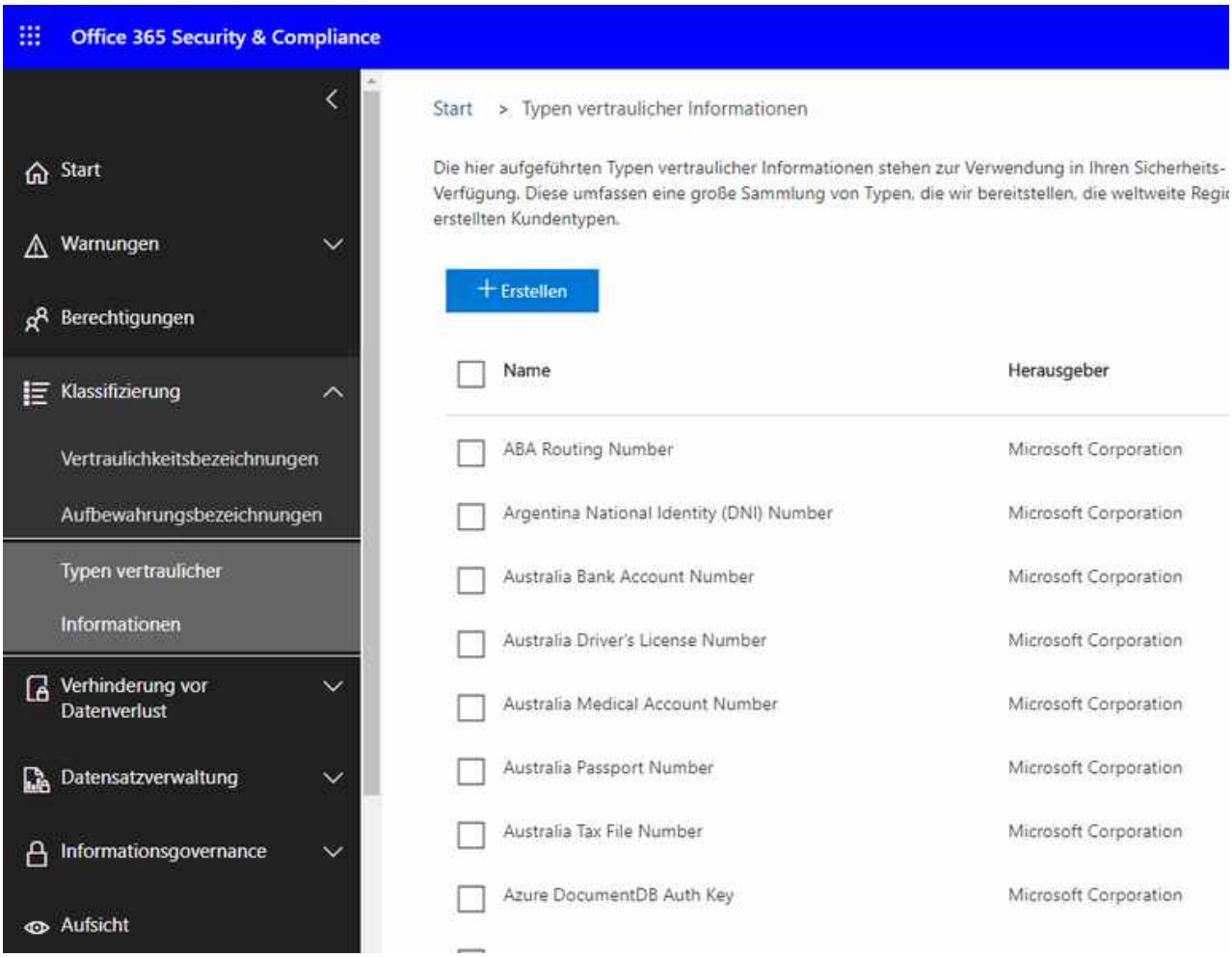
Sensibler Informationen in Dokumenten zu schützen

Angenommen, ein Mitarbeiter versucht, Dokumente mit sensiblen Informationen über den Chat in Teams zu versenden. Die DLP-Richtlinie überwacht Dateien und reagiert, wenn sie bestimmte Informationen in einem Dokument findet (z.B. die Kreditkartennummer).

Erstellen und Verwalten von DLP-Richtlinien

1. Zuerst sollten wir den "Sensible Informationen Type" für unsere DLP-Richtlinie erstellen
2. Navigieren Sie zum Microsoft 365 Sicherheits- und Compliance-Center (https://protection.office.com/)

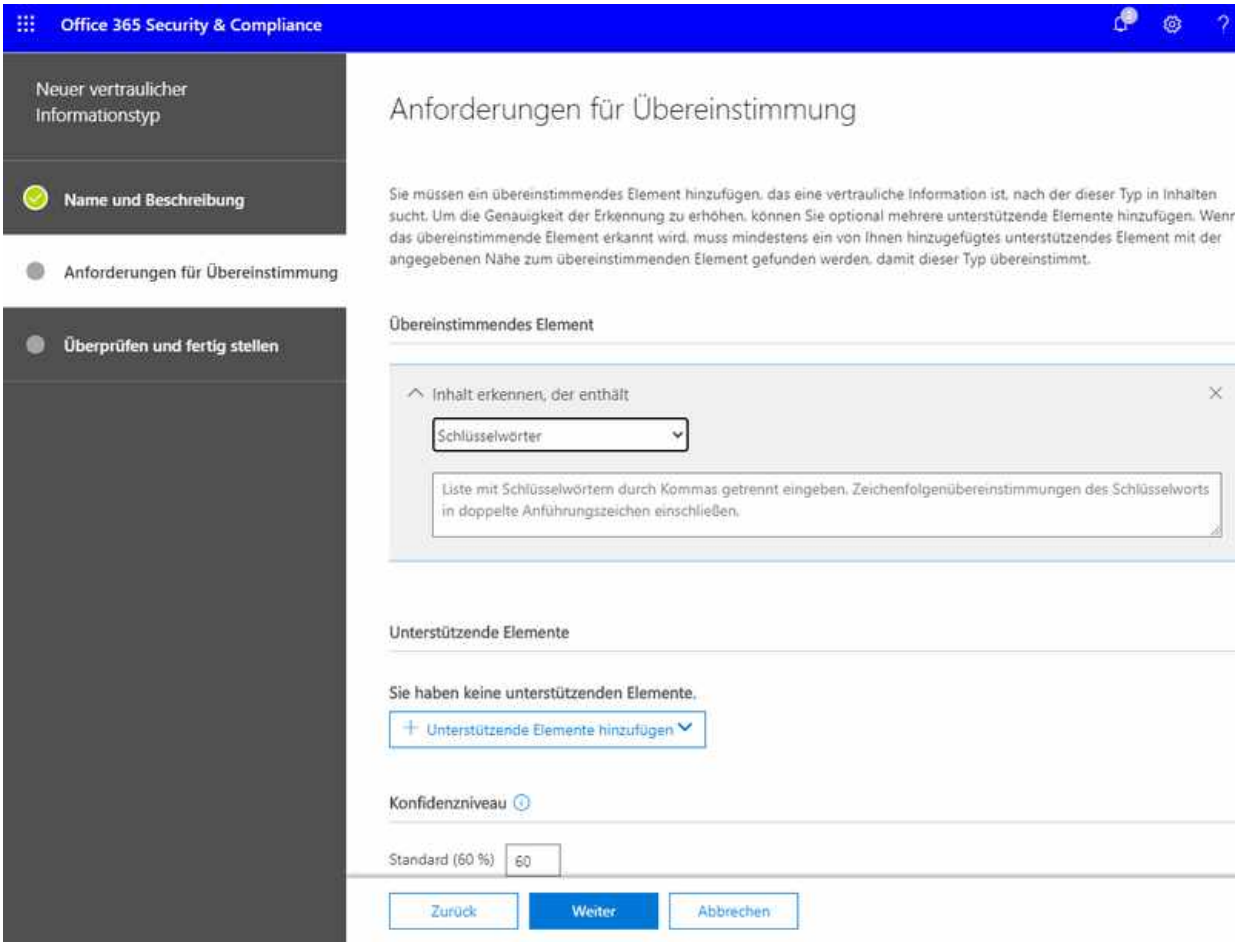
3. Klicken Sie auf **Klassifizierung > Typen vertraulicher Information**



3. Klicken Sie auf **Erstellen** und geben Sie eine **Anzeigename** und **Beschreibung** ein.

4. Bei **Anforderungen für Übereinstimmung** können wir detaillierte Regeln mit drei Arten von Erkennungsmethoden erstellen:

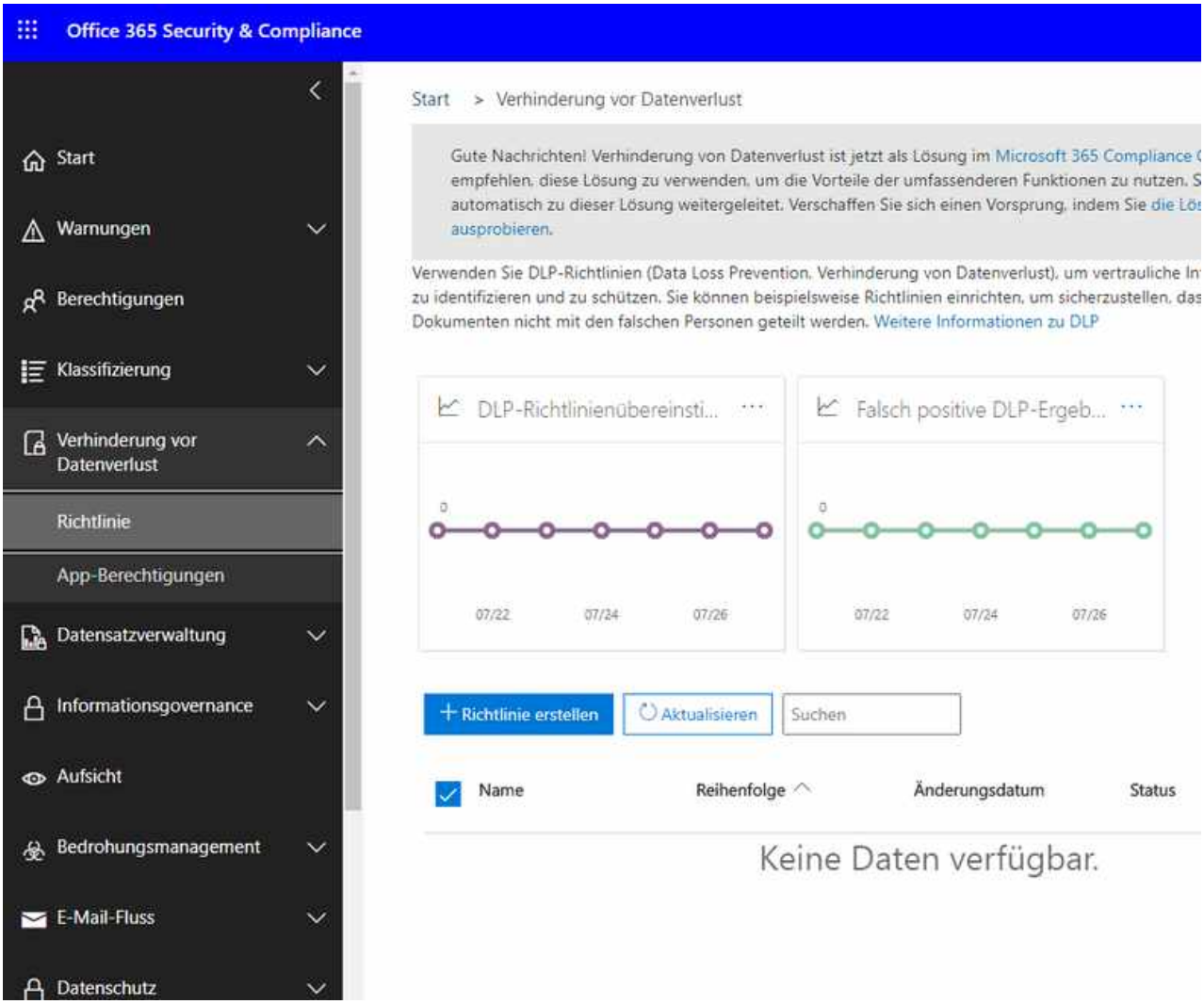
- Schlüsselwörter (Liste der Schlüsselwörter, die DLP für die Suche nach Inhalten verwendet)
- Regulärer Ausdruck (wird von DLP verwendet, um Inhalte nach Regeln abzugleichen)
- Wörterbuch (große Liste von Schlüsselwörtern)



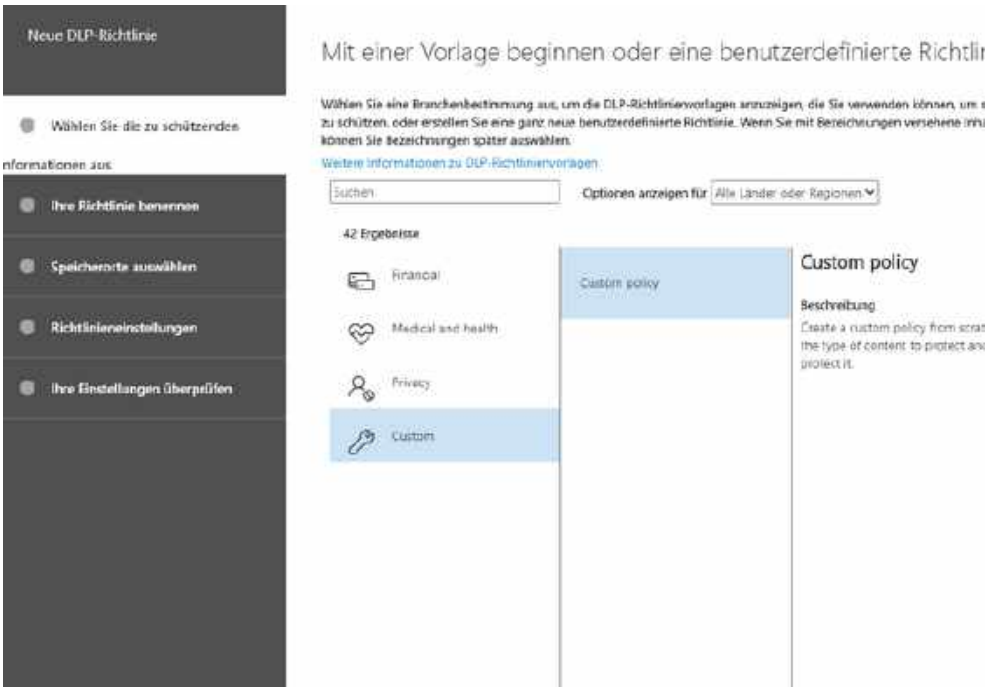
5. Wenn Sie bereit sind, **speichern** und **bestätigen** Sie den neuer vertraulicher Informationstyp.

Jetzt können wir ein neue DLP- Richtlinien erstellen.

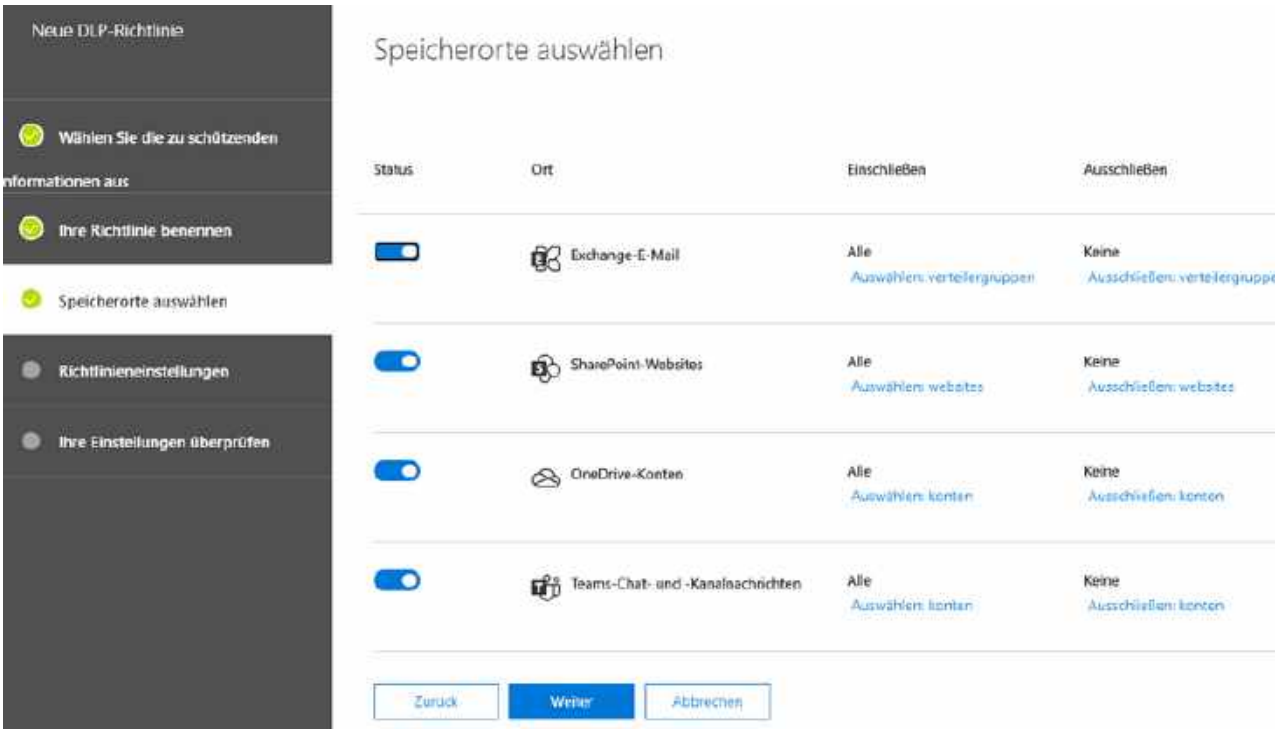
1. Navigieren Sie zum Abschnitt **Verhinderung von Datenverlusten** und wählen Sie **Richtlinie**



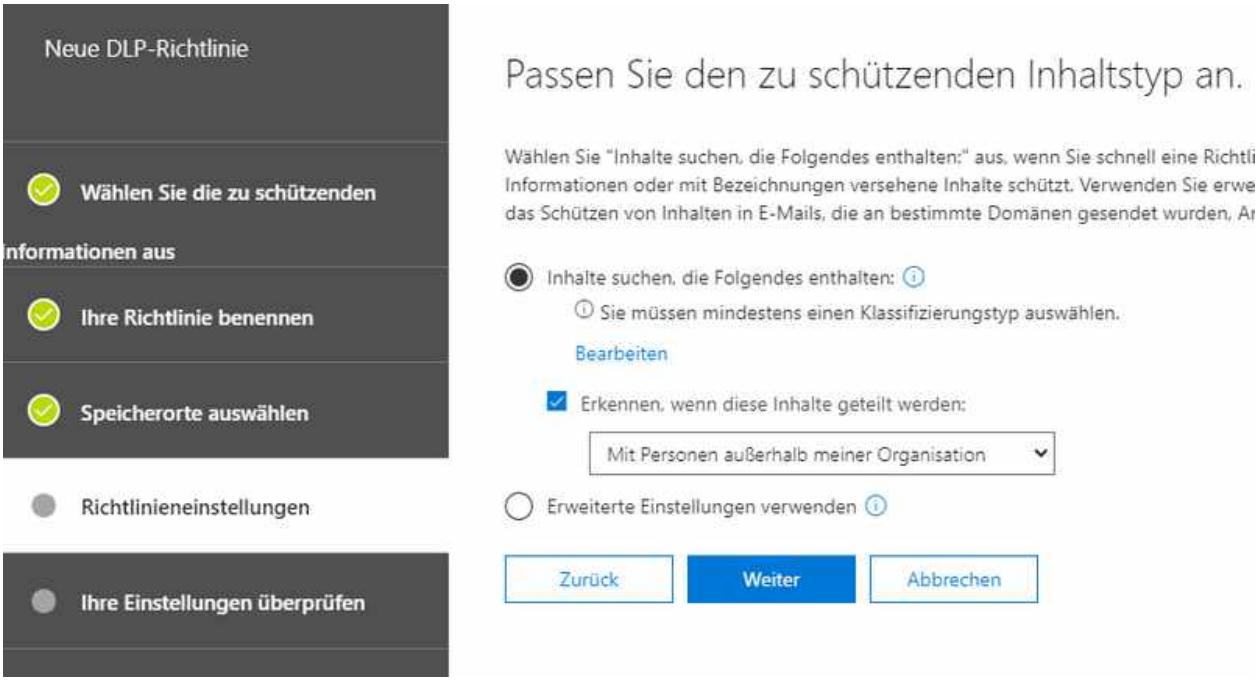
2. Klicken Sie auf **Richtlinie erstellen** und wählen Sie eine vorhandene Vorlage aus oder erstellen Sie eine benutzerdefinierte Vorlage.



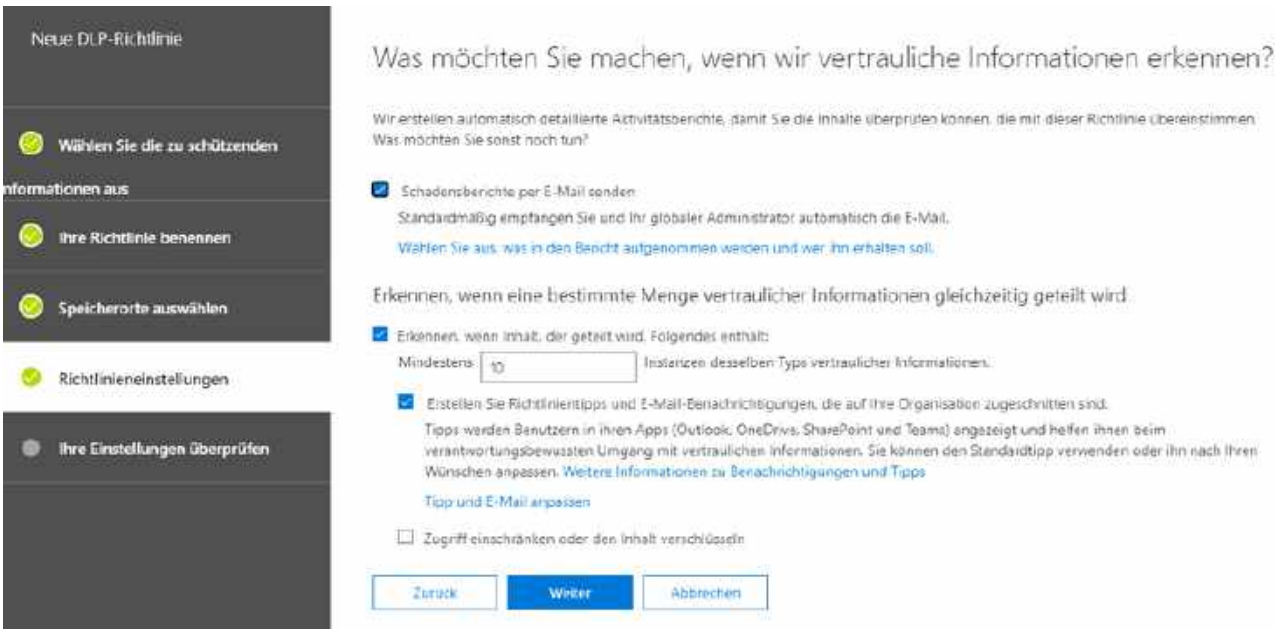
2. Unter **Speicherorte auswählen** können wir angeben, bei welchem Workloads unsere DLP-Richtlinie funktionieren soll. Wir können Exchange-E-Mail, SharePoint-Websites, OneDrive-Konten oder Team-Chat und Channel-Nachrichten auswählen.



3. Auf der Seite **Richtlinieneinstellungen** müssen wir den Typ "Sensible Informationen" auswählen. Basierend auf dieser Regel wird unsere DLP-Richtlinie versuchen, den Inhalt



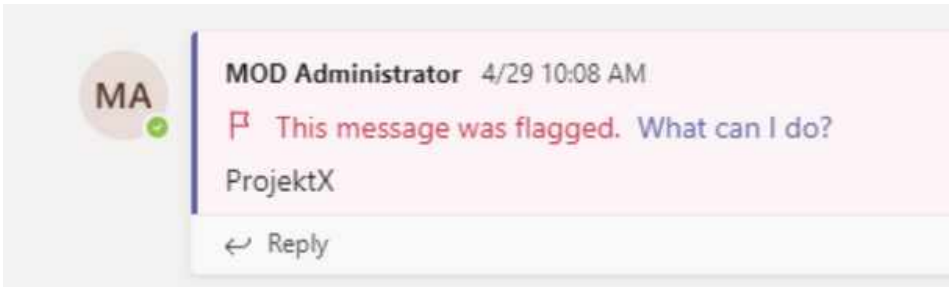
4. Am Ende können wir zusätzliche Parameter angeben (z.B. E-Mail-Benachrichtigungen, Tipps für Benutzer anzeigen, usw.)



6. Dann können wir unsere DLP-Richtlinie **speichern** und **bestätigen**.

Wenn ein Benutzer eine Chat-Nachricht oder ein Dokument mit vertraulichen Informationen sendet, wird er über den Vorfall benachrichtigt.

Chat Message Benachrichtigung



Dokument Benachrichtigung

DATEN AUSTAUSCHEN

Der Informationsaustausch mit externen Mitarbeitern oder Partnern ist ein sehr übliches Verhalten. Der Informationsaustausch ermöglicht es uns, schnell Informationen zu senden und Feedback zu erhalten, aber wir müssen uns der Vor- und Nachteile im betracht ziehen.

Gast vs. Externer Benutzer

Microsoft Teams ermöglicht es uns, mit zwei Arten von Benutzern zusammenzuarbeiten:

Gast

Ein Gastbenutzer ist jemand außerhalb Ihrer Organisation ohne ein Konto in Ihrer Organisation (z.B. Partner, Verkäufer, Berater). Der Gastbenutzer kann in ein Team eingeladen werden und innerhalb dieses Teams mit Ihnen zusammenarbeiten.

Externer Benutzer

Ein externer Nutzer ist jemand, der Teams oder Skype für Unternehmen nutzt und mit Ihrer Organisation zusammengeschlossen ist. Gäste und externe Benutzer haben unterschiedliche Fähigkeiten, wenn sie mit Ihnen in Teams arbeiten.

Externe Benutzer können im Teams Admin Center im Abschnitt **Externer Zugriff** konfiguriert werden.

https://admin.teams.microsoft.com/company-wide-settings/external-communications

Gastbenutzer können im Teams Admin Center im Abschnitt **Gastzugang** konfiguriert werden.

https://admin.teams.microsoft.com/company-wide-settings/external-communications

MEET THE AUTHOR

Zachary Woods

Ich bin ein Power Platform and Dynamics 365 Berater. Ich entwickle Anwendungen und Lösungen, die die Produktivität mit der Power Platform, Sharepoint und Teams verbessern und erleichtern. Ich bin ein großer Fan von Prozessautomatisierung und der Implementierung von Modern Workplace Tools. Ich bin ein amerikanischer "Ex-Pat", der derzeit mit meiner Frau und meiner Tochter in Würzburg, Deutschland, wohnt. Ich lese gerne und interessiere mich für Themen wie Psychologie, Philosophie, Finanzen und Investieren.