


# DATEN- KLASSIFIZIERUNG

---

Den Schutzbedarf für Klassifizierungsstufen definieren,  
Risikokategorien identifizieren und Regeln  
zur Klassifizierung von strukturierten oder  
unstrukturierten Daten aufstellen.

Um Ihre sensiblen Daten schützen zu können, müssen Sie wissen, welche Daten sensibel sind und wo sie liegen. Datenklassifizierung ist der Prozess, in dem strukturierte oder unstrukturierte Daten analysiert und aufgrund des Dateityps und des Inhalts in Kategorien eingeordnet werden. Klassifizierungen haben verschiedene Stufen, die zum Beispiel „intern“, „vertraulich“, „streng vertraulich“ oder „öffentlich“ lauten könnten. Im Zuge eines gemeinsamen Workshops wird eine Klassifizierungsrichtlinie erstellt und der Schutzbedarf für die Klassifizierungsstufen definiert. Außerdem werden Risikokategorien identifiziert und Regeln für die Klassifizierung von Informationen aufgestellt.

---



**DURCH DIE KLASSIFIZIERUNG MIT AZURE INFORMATION PROTECTION KÖNNEN SIE IHRE DATEN ÜBER UNTERNEHMENSGRENZEN HINWEG SICHERN UND ERHALTEN ZUSÄTZLICH DIE MÖGLICHKEIT FÜR DEN SCHUTZ DER GESAMTEN E-MAIL-KOMMUNIKATION.**

PETER ROSENDAHL, DIRECTOR SOLUTIONS,  
CYBERSECURITY, CLOUD ARCHITECTURE & NEW WORK,  
ALL FOR ONE GROUP SE

---

---

### **KLASSIFIZIERUNGSRICHTLINIEN HABEN ZUM ZIEL:**

- Bereitstellung eines Informations-Inventars von klassifizierten Informationen
- Bewusstseinsbildung auf Seiten der Informationseigentümer bezüglich des Eigentums klassifizierter Informationen und der Verantwortung für diese
- Erklärung der für klassifizierte Informationen relevanten Rollen und Verantwortlichkeiten
- Definition der Vertraulichkeitsstufen und Klassifizierungskriterien
- Befähigung des Informationseigentümers zur eigenständigen Anwendung der Klassifizierungsmethode sowie zur laufenden Aktualisierung seines Bestands an klassifizierten Informationen

---

### **DER GRUNDSÄTZLICHE KLASSIFIZIERUNGSPROZESS:**

- Beschreibt sich im sogenannten PDCA-Zyklus mit den folgenden Phasen: Plan, Do, Check und Act
- Bei diesem Prozess handelt es sich um einen Zyklus und nicht um einen Ablauf
- Die Klassifikation sollte ständig überprüft und den Unternehmensumständen angepasst werden

**DIE EINZELNEN PROZESSCHRITTE  
ZUR KLASSIFIZIERUNG:**

---

**PLAN**

Identifizierung der Datenbestände, Ernennung eines Informations-Verantwortlichen (ggf. Datenschutzbeauftragten), sowie Entwicklung eines Rahmenwerks bestehend aus Schutzklassen und Richtlinien.

---

**DO**

Nachdem die Schutzklassen und Richtlinien abgestimmt wurden, ist das Deployment der Schutztechnologie. Im gleichen Zuge werden die definierten Schutzklassen und Richtlinien implementiert und durchgesetzt.

---

**CHECK**

Validierung und Überprüfung der definierten Richtlinien und Schutzklassen gegen den Erfüllungsgrad des ursprünglich gedachten Zwecks.

---

**ACT**

Reklassifizierung von Daten und Dateien, um sich an Änderungen und neue Risiken anzupassen.

**INHALTE DES WORKSHOPS ZUR  
DATENKLASSIFIZIERUNG**

---

⌘ Darstellung einer Klassifizierungstaxonomie und Hierarchie

---

⌘ Welche Datenklassifizierung gibt es bereits im Unternehmen?

---

⌘ Ermitteln von Sensitivitätsstufen von Daten, die in der Organisation vorhanden sind

---

⌘ Design, Definition „Use Scoped“ Policies für bestimmte Teams/Fachabteilungen

---

⌘ Entwerfen eines Blueprints als Enterprise-Template für weitere Fachabteilungen

---

⌘ Definition der Label-Bezeichnungen

---

⌘ Identifizierung, welche Schutzmaßnahmen für Ihre Organisation erforderlich sind

---

⌘ Konvertierung der Anforderungen in Business Use Cases

## **IHRE VORTEILE**

- 
- ⌘ Gemeinsames Erarbeiten einer Klassifizierungsrichtlinie als Grundlage für einen unternehmensweiten Standard im Umgang mit sensiblen Daten
- 
- ⌘ Identifizieren von sensiblen Dateien, geistigem Eigentum und Geschäftsgeheimnissen
- 
- ⌘ Identifizieren von regulierten Daten, um die Anforderungen von Vorschriften wie beispielsweise HIPAA, PCI DSS oder DSGVO zu erfüllen
- 
- ⌘ Erkennen statistisch signifikanter Muster oder Trends im Datenbestand
- 
- ⌘ Basis für die Umsetzung einer Label- und Klassifizierungstechnologie wie beispielsweise Azure Information Protection (AIP) ist geschaffen

## **UNSERE LEISTUNGEN**

- 
- ⌘ Ganztätiger Workshop, durchgeführt von einem erfahrenen Security-Architekten und einem Cybersecurity-Berater
- 
- ⌘ Gemeinsame Erstellung einer Klassifizierungsrichtlinie von Informationen
- 
- ⌘ Ergebnisse des Workshops werden in einem Konzept zusammengefasst
- 
- ⌘ Vorlage zur Klassifizierung von Daten und Bestimmung des Schutzbedarfes wird zur Verfügung gestellt

---

**DIE DATENKLASSIFIZIERUNG AUF BASIS EINER KLASSIFIZIERUNGSRICHTLINIE IST GANZ EINFACH: IM ERSTEN SCHRITT ERSTELLEN SIE UNTERSCHIEDLICHE KATEGORIEN MIT DEN GEWÜNSCHTEN VERTRAULICHKEITSSTUFEN. ANSCHLIESSEND WEISEN SIE IHRE DATEN DIESEN KATEGORIEN ZU. FALLS NOCH KEINE KLASSIFIZIERUNGSRICHTLINIE VORHANDEN SEIN SOLLTE, UNTERSTÜTZEN WIR GERNE MIT EINER GRUNDSTRUKTUR.**

**All for One Group AG**

Rita-Maiburg-Str. 40  
70794 Filderstadt

Roland Dühning  
Senior Sales Manager

---

☎ +49 151 52642 338

✉ [cc@all-for-one.com](mailto:cc@all-for-one.com)

**CC.ALL-FOR-ONE.COM**