Consulting Briefing · 17.11.2026 · boddenberg.de

Security & Compliance

Purview: Sensitivity Labels für Entra-Sicherheitsgruppen, Rollout ab Mitte Januar 2027

Executive Summary

Sicherheitsgruppen sind der Schlüsselbund deines Mandanten. Sie entscheiden, wer in welche App darf, wen eine Conditional-Access-Richtlinie trifft und wer auf welche Azure-Ressource zugreift. Ausgerechnet dort gab es bisher keine Vertraulichkeitsbezeichnungen, die gab es nur für Microsoft-365-Gruppen, Teams und SharePoint-Websites. Laut Microsoft-Ankündigung MC1508238 ändert sich das: **Ab Mitte Januar 2027 lassen sich veröffentlichte Purview-Sensitivity-Labels weltweit auch Cloud-Sicherheitsgruppen in Microsoft Entra ID zuweisen.** Das Label setzt dann Regeln für Mitgliedschaft und Gastzugriff durch, beim Anlegen der Gruppe, bei der ersten Zuweisung und bei jedem neuen Mitglied.

Microsoft hat die Meldung am 13. November 2026 überarbeitet. In Fassung 2 rutscht der Termin von Mitte bis Ende November 2026 auf **Mitte Januar 2027**. Zwei Dinge musst du dir merken. Erstens ist die Funktion **standardmäßig aus** und braucht einen eigenen Schalter, auch wenn Labels für Microsoft-365-Gruppen bei dir längst laufen. Zweitens ist ein **einmal zugewiesenes Label derzeit weder änderbar noch entfernbar**. Es ist also eher ein Tattoo als ein Aufkleber. Wer im Januar aus Neugier den Schalter umlegt und die halbe Gruppenlandschaft mit „Vertraulich“ beklebt, darf sich anschließend eine neue Gruppenlandschaft bauen.

Wichtig: Unsere Empfehlung in einem Satz

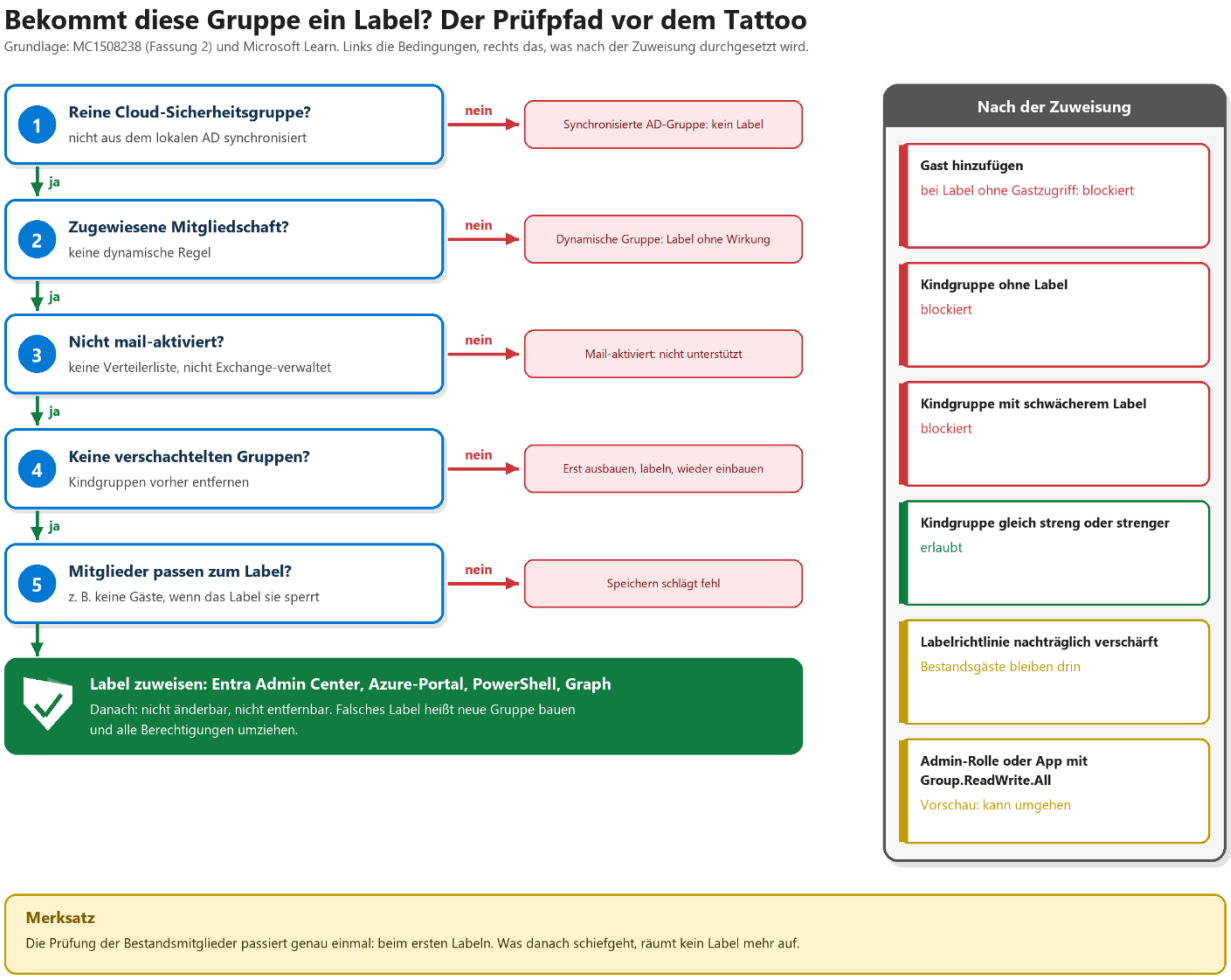
Schalte die Funktion erst ein, wenn die Labeltaxonomie für Gruppen eingefroren, der Betriebs- oder Personalrat unterrichtet und ein Pilot mit dem Identity-Team gelaufen ist. Für alles davor reichen die acht Wochen, die Microsoft dir gerade geschenkt hat.

Worum geht es im Detail?

Zuerst die Hintergründe. Eine **Microsoft-365-Gruppe** ist ein Kollaborationsobjekt: Postfach, Team, SharePoint-Website, Planner. Labels für solche Container kennst du seit Jahren. Sie steuern Privatsphäre, Gastzugriff, externes Teilen und den Zugriff von nicht verwalteten Geräten. Eine **Sicherheitsgruppe** ist etwas anderes. Microsoft Learn nennt sie ein Autorisierungsprimitiv, also ein Sicherheitsprinzipal, das Entra ID und nachgelagerte Systeme bei jeder Zugriffsentscheidung auswerten. Ihre Mitgliederliste ist ein Bündel von Berechtigungen. Wer in „SG-ERP-Finanzbuchhaltung“ steht, sieht Zahlen. Wer in „SG-CA-Ausnahme-MFA“ steht, kommt ohne zweiten Faktor durch.

Genau deshalb ist Microsoft bei Sicherheitsgruppen streng. Verbietet ein Label Gäste, muss Entra ID die **effektive Mitgliedschaft** prüfen, also auch alle Mitglieder, die über verschachtelte Gruppen hereinkommen. Diese Prüfung findet laut Microsoft Learn heute nur bei der Erstellung der Gruppe und bei der ersten Labelzuweisung statt. Ein Wechsel des Labels müsste die ganze

Hierarchie neu bewerten, und das kann Entra noch nicht. Daher die Unveränderlichkeit. Fassung 2 von MC1508238 spricht weiterhin von „derzeit“ und kündigt die Änderbarkeit für ein späteres Update an. Rechne also nicht damit, dass sie zum Start im Januar schon da ist.



Die Grafik zeigt, wie eng das Nadelöhr ist. **Nicht unterstützt** werden aus dem lokalen Active Directory synchronisierte Gruppen, Gruppen mit dynamischer Mitgliedschaft, mail-aktivierte Sicherheitsgruppen und Verteilerlisten. In einem typischen Hybrid-Mittelstand fällt damit schon die Hälfte der Gruppen raus. Wer eine Gruppe mit verschachtelten Kindgruppen labeln will, muss die Kinder erst entfernen, den Elternteil labeln, die Kinder mit einem gleich strengen oder strengeren Label versehen und dann wieder einhängen. Zugewiesen wird über das Entra Admin Center, das Azure-Portal, PowerShell oder Microsoft Graph. Das Microsoft 365 Admin Center und das Portal „Meine Gruppen“ können es nicht.

Verhalten	Microsoft-365-Gruppe	Cloud-Sicherheitsgruppe
Label ändern oder entfernen	Jederzeit durch Besitzer oder Admin	**Nicht möglich**, Label ist fest
Verschachtelung	Gibt es nicht	Erlaubt, Kindgruppe muss gleich streng oder strenger gelabelt sein
Prüfung der Bestandsmitglieder	Nur neue Mitglieder	Neue Mitglieder plus einmalige Gastprüfung bei der ersten Zuweisung
Admin-Rollen	Halten sich an die Labelrichtlinie	Vorschau: zahlreiche Admin-Rollen und Apps können umgehen
Aktivierung	Vorlage Group.Unified, EnableMIPLabels	Eigene Vorlage Group.Security, EnableMIPLabels
Unterstützte Typen	Alle Microsoft-365-Gruppen	Nur Cloud-Gruppen mit zugewiesener Mitgliedschaft, nicht mail-aktiviert

Fakten: So wird der Schalter umgelegt

Lizenz: mindestens eine aktive Entra-ID-P1-Lizenz im Mandanten, enthalten etwa in Microsoft 365 E3, E5 und Business Premium. **Labels:** im Purview-Portal mit dem Bereich „Gruppen und Websites“ anlegen und veröffentlichen, dann in der Security-&-Compliance-PowerShell **Execute-AzureADLabelSync** ausführen und bis zu 24 Stunden warten. **Mandant:** in der Microsoft-Graph-PowerShell (Beta-Modul) eine Verzeichniseinstellung auf Basis der Vorlage **Group.Security** anlegen oder anpassen und **EnableMIPLabels** auf True setzen. Die bestehende Einstellung für Microsoft-365-Gruppen hilft dir dabei nicht, beide Gruppentypen laufen über getrennte Vorlagen.

Was sind Chancen? Was sind Risiken?

Die Chance ist größer, als sie klingt. Ein Beispiel aus einem Maschinenbauer mit 600 Köpfen: Bei einem Berechtigungs-Review fanden wir in der Sicherheitsgruppe für den Finanzbereich des ERP einen Gast, den externen Steuerberater. Den hatte jemand 2023 „nur für den Jahresabschluss“ hinzugefügt. Der Jahresabschluss ist lange durch, der Steuerberater inzwischen im Ruhestand, das Konto lebte noch. Ein Label „Vertraulich – nur intern“ hätte diesen Gast zwar nicht entfernt. Aber die erste Zuweisung wäre gescheitert, und genau dieses Scheitern ist der Befund, den du willst. Danach kommt kein Gast mehr hinein, auch nicht freitags um 17 Uhr.

Dazu kommen einheitliche Klassifizierung über alle Gruppentypen hinweg, kontrollierte Self-Service-Gruppenerstellung und Nachweise für ISO 27001 oder NIS2. Wer dem Auditor zeigen kann, dass kritische Berechtigungsgruppen technisch gastfrei bleiben, gewinnt Zeit für die wirklich unangenehmen Fragen.

Jetzt das Risiko. Das größte heißt **Unveränderlichkeit**. Hängt das falsche Label an einer Gruppe, empfiehlt Microsoft Learn ganz trocken: neue Gruppe anlegen, Mitglieder neu hinzufügen. Was dort nicht steht: Jede App-Rollenzuweisung, jede Conditional-Access-Ausnahme, jede Azure-RBAC-Zuweisung, jede SharePoint-Berechtigung und jedes Lizenzgruppen-Mapping, das an der alten Objekt-ID hängt, musst du nachziehen. Das ist wie ein Umzug mit Kindern: Alle sind sicher, nichts vergessen zu haben, und drei Wochen später fehlt der Zugang zur Lohnbuchhaltung.

Warnung: Das Label ist kein Türsteher für Admins

Microsoft Learn führt die Funktion noch als Vorschau und listet Rollen, die die Labelrichtlinie beim Hinzufügen von Mitgliedern **umgehen** können: unter anderem Global Administrator, User Administrator, Groups Administrator, Exchange-, SharePoint- und Teams-Administrator sowie Helpdesk Administrator. Dazu kommen Apps mit Group.ReadWrite.All, Directory.ReadWrite.All oder GroupMember.ReadWrite.All. Das ist praktisch jedes Provisionierungswerkzeug, das du hast. Microsoft stellt in Aussicht, dass sich das bis zur allgemeinen Verfügbarkeit ändert. Bis du es selbst getestet hast, ist das Label ein Schild an der Tür, kein Schloss.

Zwei weitere Fallen. Verschärfst du später ein Label in Purview, etwa von „Gäste erlaubt“ auf „Gäste gesperrt“, bleiben vorhandene Gäste in allen bereits gelabelten Gruppen drin, bis jemand sie entfernt. Und löschst du ein Label, das noch in einer Richtlinie steckt, scheitert laut Microsoft Learn die Erstellung neuer Gruppen und Websites. Die Labeltaxonomie für Gruppen wird damit zum Grundgesetz: selten ändern, nie spontan.

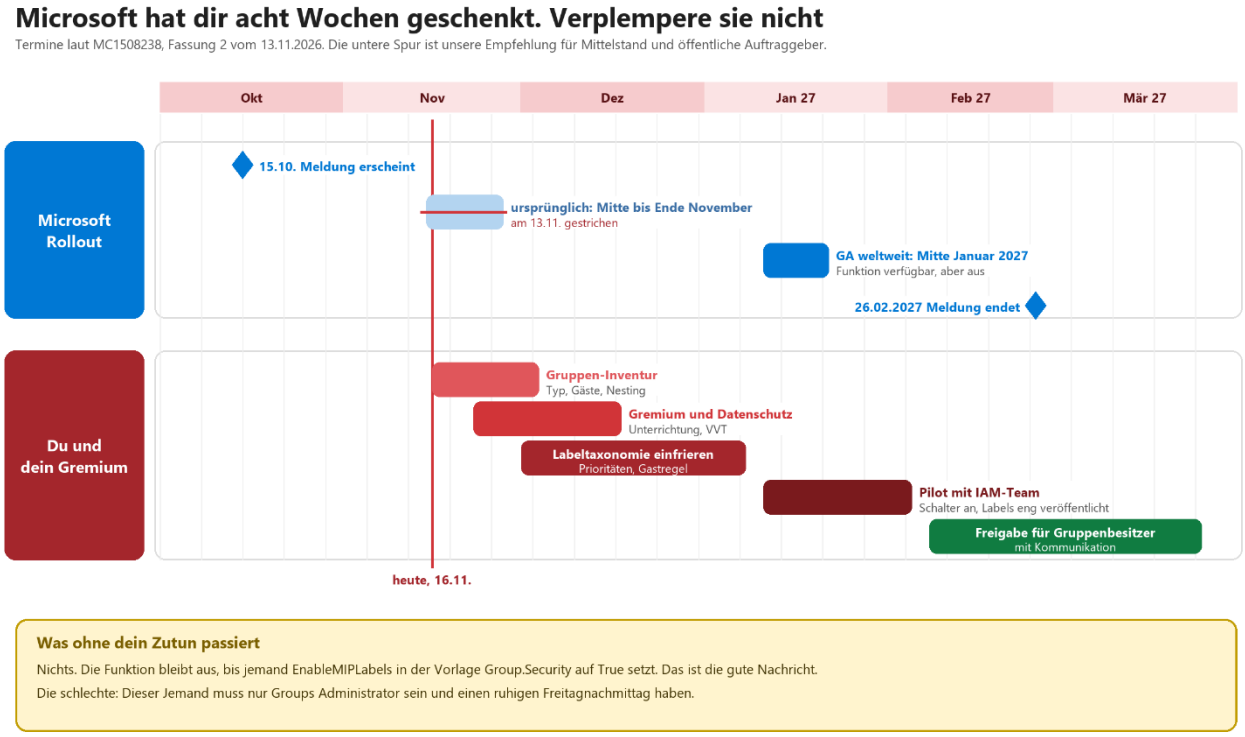
Zum **Datenschutz**: Das Label selbst verarbeitet kaum personenbezogene Daten. Neu sind aber Audit-Ereignisse in Purview. Wer welches Label gesetzt hat und wessen Hinzufügen abgelehnt wurde, steht mit Name und Zeitstempel im Protokoll. Für das Verzeichnis der Verarbeitungstätigkeiten reicht meist eine Ergänzung beim bestehenden Eintrag für Entra ID und Purview.

Zur **Mitbestimmung**: Nach **§ 87 Abs. 1 Nr. 6 BetrVG** genügt, dass eine technische Einrichtung objektiv geeignet ist, Verhalten oder Leistung zu überwachen. Entra und Purview sind das ohnehin, und die meisten Betriebe haben dafür eine Rahmenvereinbarung. Ob die neue Funktion darunter fällt, hängt davon ab, ob die Vereinbarung Funktionen und Auswertungen abschließend aufzählt. Ist das so, brauchst du eine Ergänzung der Anlage, bevor du einschaltest. Dazu kommt ein handfester Punkt: Labels sperren Gäste, und Gäste sind oft externe Dienstleister, Leiharbeitnehmer oder Kolleginnen und Kollegen aus Schwestergesellschaften, die über B2B angebunden sind. Wenn sich Arbeitsabläufe ändern, will das Gremium das vorher wissen. Bei öffentlichen Auftraggebern gilt Entsprechendes nach **§ 80 Abs. 1 Nr. 21 BPersVG** oder dem jeweiligen Landespersonalvertretungsgesetz.

Chance	Risiko
Gastfreiheit kritischer Berechtigungsgruppen technisch erzwingen	Falsches Label nur durch Neuaufbau der Gruppe zu korrigieren
Erste Zuweisung deckt Altlasten wie vergessene Gäste auf	Admin-Rollen und Provisionierungs-Apps umgehen die Regel (Vorschau)
Eine Taxonomie für Microsoft-365-Gruppen und Sicherheitsgruppen	Spätere Richtlinienänderungen wirken nicht auf Bestandsmitglieder
Kontrollierte Self-Service-Gruppenerstellung	Synchronisierte, dynamische und mail-aktivierte Gruppen bleiben außen vor
Belastbare Nachweise für ISO 27001 und NIS2	Gelöschte Labels blockieren das Anlegen neuer Gruppen

Was müssen wir jetzt schon vorbereiten?

Weil nichts automatisch passiert, ist das hier eine Planungsaufgabe, keine Feuerwehrübung. Genau das macht sie gefährlich. Planungsaufgaben ohne Termin erledigen sich in der IT bekanntlich am Tag nach dem Vorfall.



Bis 04.12.2026 – Gruppen-Inventur. Exportiere per Microsoft Graph alle Sicherheitsgruppen mit Quelle (Cloud oder synchronisiert), Mitgliedschaftstyp, Mail-Aktivierung, Anzahl der Gäste und verschachtelten Kindgruppen. Markiere die Gruppen, die Zugriff auf Kronjuwelen steuern: Finanzen, Personal, Conditional-Access-Ausnahmen, privilegierte Azure-Ressourcen. Nur dort lohnt sich ein Label in der ersten Welle.

Bis 18.12.2026 – Gremium und Datenschutz. Unterrichte den Betriebs- oder Personalrat schriftlich: was das Label durchsetzt, welche Audit-Ereignisse entstehen, wer sie auswerten darf und welche externen Personen betroffen sein können. Prüfe, ob die IT-Rahmenvereinbarung eine Anlage braucht, und ergänze das Verzeichnis der Verarbeitungstätigkeiten.

Bis 08.01.2027 – Labeltaxonomie einfrieren. Prüfe deine Labels mit Bereich „Gruppen und Websites“. Weil Kindgruppen gleich streng oder strenger gelabelt sein müssen, entscheidet die **Prioritätsreihenfolge** der Labels plötzlich über Berechtigungen. Lege fest, welches Label Gäste sperrt, und ändere diese Einstellung danach nicht mehr. Bereite ein Skript vor, das eine falsch gelabelte Gruppe samt Mitgliedern, Besitzern und Zuweisungen neu aufbaut. Du wirst es brauchen.

Tipp: Erst eng veröffentlichen, dann öffnen

Das Entra Admin Center zeigt nur die Labels, die in einer für dich geltenden Veröffentlichungsrichtlinie stehen. Nutze das: Veröffentliche die Gruppenlabels zuerst ausschließlich für das Identity-Team. Dann kann kein Gruppenbesitzer im Januar aus Versehen ein Tattoo stechen, während du noch testest.

Ab Mitte Januar 2027 – Pilot. Setze EnableMIPLabels in der Vorlage Group.Security, synchronisiere die Labels und warte die 24 Stunden ab. Lege neue Testgruppen an, statt produktive Gruppen zu labeln. Prüfe gezielt, ob deine Admin-Konten und Provisionierungs-Apps die Gastsperre noch umgehen. Die Antwort entscheidet, ob du zusätzlich Zugriffsüberprüfungen oder Warnungen brauchst.

Ab Februar 2027 – Freigabe und Kommunikation. Öffne die Labels für Gruppenbesitzer erst nach dem Pilot, mit einer kurzen Anleitung: Welches Label wofür, warum es endgültig ist und wen man vorher fragt. Die Belegschaft insgesamt merkt wenig. Betroffen sind vor allem Gruppenbesitzer und die Fachbereiche, die mit Externen arbeiten.

Wann	Was	Wer
bis 04.12.2026	Sicherheitsgruppen inventarisieren, Kronjuwelen markieren	Identity-Team
bis 18.12.2026	Betriebs- oder Personalrat unterrichten, Rahmenvereinbarung prüfen	IT-Leitung, Personalabteilung
bis 18.12.2026	Verzeichnis der Verarbeitungstätigkeiten ergänzen	Datenschutz
bis 08.01.2027	Labeltaxonomie und Prioritäten festschreiben, Neuaufbau-Skript	Purview-Administration
ab Mitte Januar 2027	Schalter setzen, Pilot mit Testgruppen, Admin-Umgehung testen	Identity-Team, Security
ab Februar 2027	Labels für Gruppenbesitzer veröffentlichen, Anleitung verteilen	Identity-Team, Kommunikation

Die Einrichtung beschreibt Microsoft unter Zuweisen von Vertraulichkeitsbezeichnungen zu Microsoft Entra-Sicherheitsgruppen, die Labeleinstellungen für Container unter Verwenden von Vertraulichkeitsbezeichnungen zum Schutz von Gruppen und Websites. Den aktuellen Stand des Rollouts zeigt der Eintrag 568217 in der Microsoft 365 Roadmap.

Weiterlesen › Entra ID unterstützt Purview Sensitivity Labels

Weiterlesen › Entra Connect Sync wird durch Cloud Sync abgelöst

Häufig gestellte Fragen

Ab wann gibt es Sensitivity Labels für Entra-Sicherheitsgruppen?

Laut Microsoft-Ankündigung MC1508238 in der überarbeiteten Fassung vom 13. November 2026 beginnt die weltweite allgemeine Verfügbarkeit Mitte Januar 2027 und soll noch im Januar abgeschlossen sein. Ursprünglich war Mitte bis Ende November 2026 geplant.

Kann man ein Sensitivity Label von einer Sicherheitsgruppe wieder entfernen?

Nein, derzeit lässt sich ein Label auf einer Cloud-Sicherheitsgruppe weder ändern noch entfernen. Microsoft empfiehlt, bei einem falschen Label eine neue Gruppe mit dem richtigen Label anzulegen

und die Mitglieder dorthin zu übertragen. Alle Berechtigungen der alten Gruppe müssen dabei nachgezogen werden.

Reicht die Aktivierung von Labels für Microsoft-365-Gruppen auch für Sicherheitsgruppen?

Nein, Sicherheitsgruppen nutzen die eigene Verzeichnisvorlage Group.Security, in der EnableMIPLabels separat auf True gesetzt werden muss. Die Einstellung in Group.Unified für Microsoft-365-Gruppen wirkt nicht auf Sicherheitsgruppen.

Welche Sicherheitsgruppen können kein Sensitivity Label bekommen?

Ausgeschlossen sind aus dem lokalen Active Directory synchronisierte Gruppen, Exchange-verwaltete und mail-aktivierte Sicherheitsgruppen, Verteilerlisten sowie Gruppen mit dynamischer Mitgliedschaft. Gruppen mit verschachtelten Kindgruppen lassen sich erst labeln, wenn die Kindgruppen vorübergehend entfernt wurden.

Muss der Betriebsrat vor der Einführung von Labels für Sicherheitsgruppen beteiligt werden?

Wenn die bestehende Vereinbarung zu Entra ID und Purview die Funktionen abschließend aufzählt, ist eine Ergänzung nach § 87 Abs. 1 Nr. 6 BetrVG in der Regel nötig, weil neue Audit-Ereignisse mit Personenbezug entstehen. Zusätzlich sollte das Gremium erfahren, wenn die Gastsperre die Zusammenarbeit mit externen Personen verändert.