# Dokumentenklassifizierung im Rahmen der ISO 27001

Die ISO 27001 ist ein internationaler Standard für Informationssicherheitsmanagement, der Unternehmen hilft, Risiken im Umgang mit sensiblen Daten zu minimieren.
Bei der **Dokumentenklassifizierung** im Rahmen der **ISO 27001** geht es darum, Informationen systematisch zu bewerten und in Kategorien einzuteilen, um sie vor unbefugtem Zugriff oder Missbrauch zu schützen.

## Warum wird klassifiziert?

Informationen in einem Unternehmen haben unterschiedliche Grade an Vertraulichkeit und Wichtigkeit. Um sie entsprechend zu schützen, wird eine Klassifizierung vorgenommen. Diese Klassifizierung bestimmt, wie ein Dokument gehandhabt, gespeichert und weitergegeben werden darf. Die Kategorien reichen typischerweise von **"öffentlich"** bis **"streng vertraulich"**.
Jede Stufe hat eigene Sicherheitsanforderungen.

### Klassifikationsstufen im Detail

1. **Öffentlich**: Informationen, die für jeden zugänglich sind, z.B. auf der Unternehmenswebsite.
2. **Intern**: Informationen, die nur für Mitarbeiter bestimmt sind, aber keinen hohen Schutz erfordern.
3. **Vertraulich**: Sensible Informationen, die nur einem begrenzten Personenkreis zugänglich sein dürfen.
4. **Streng vertraulich**: Kritische Informationen, deren Verlust oder Offenlegung große Schäden verursachen könnte.

## Regeln für den Umgang mit Dokumenten

Die Klassifizierung legt auch fest, **was mit den Dokumenten gemacht werden darf** und was nicht. Zum Beispiel:

- **Speichern**: Streng vertrauliche Dokumente müssen oft verschlüsselt und in gesicherten Umgebungen aufbewahrt werden.
- **Zugriff**: Nur autorisierte Personen dürfen auf bestimmte Dokumente zugreifen. Dies wird durch Zugriffsrechte gesteuert.
- **Weitergabe**: Je nach Klassifizierung dürfen Dokumente nur bestimmten Empfängern oder gar nicht weitergegeben werden.
- **Löschen**: Einige Dokumente müssen nach einem bestimmten Zeitraum sicher gelöscht oder archiviert werden.

Diese Maßnahmen helfen Unternehmen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten und das Risiko von Datenverlust oder -missbrauch zu minimieren. Die ISO 27001 schreibt vor, dass diese Prozesse dokumentiert und regelmäßig überprüft werden, um die Sicherheit zu gewährleisten.

## Vertraulichkeitsstufen im Detail

Alle Informationen müssen nachfolgenden Vertraulichkeitsstufen klassifiziert werden.

| ***Vertraulichkeits-stufe*** | ***Kennzeichnung*** | ***Klassifizierungs-kriterien*** | ***Zugangs-beschränkung*** | ***Beispiele*** |
|---|---|---|---|---|
| Öffentlich | ÖFFENTLICH | Die Veröffentlichung der Information würde die Organisation auf keine Weise beeinträchtigen | Information ist öffentlich verfügbar | Webseite, Success-Story |
| Intern | INTERN | Unberechtigter Zugang zur Information könnte geringere Schäden und/oder Unannehmlichkeiten für die Organisation verursachen | Information ist für alle Mitarbeiter und ausgesuchte Dritte verfügbar | Rechnungen, Angebote, |

| | | | | |
|---|---|---|---|---|
| Vertraulich | VERTRAULICH / NICHT GEKENNZEICHNET | Unberechtigter Zugang zur Information könnte erheblichen Schaden für das Geschäft und/oder das Ansehen der Organisation verursachen | Information ist nur einer spezifischen Gruppe von Mitarbeitern und autorisierten Dritten zugänglich | IT-Dokumentation, Gehaltsdaten, Lohnzettel |
| Streng vertraulich | STRENG VERTRAULICH | Unberechtigter Zugang zur Information könnte katastrophalen (irreparablen) Schaden für das Geschäft und/oder das Ansehen der Organisation verursachen | Information ist nur einzelnen Mitarbeitern der Organisation zugänglich | Ganz besonders schützenswerte Informationen, Patente, Prototypenpläne |

Um unnötige Kosten für den Schutz von Informationen zu vermeiden, gilt die Grundregel, dass die niedrigste Vertraulichkeitsstufe genutzt wird, die einen geeigneten Schutz bietet.

## Kennzeichnung von Information

Die Kennzeichnung mit Vertraulichkeitsstufen wird folgendermaßen durchgeführt:

- **Papierdokumente** – die Vertraulichkeitsstufe wird z.B. in der oberen rechten Ecke des Dokuments angegeben

- **Elektronische Dokumente** - die Vertraulichkeitsstufe wird z.B. in der oberen rechten Ecke jeder Seite des Dokuments angegeben

- **Elektronische Datenträger** (Speichermedium, USB-Stick, etc.) - die Vertraulichkeitsstufe muss auf der Oberfläche eines solchen Mediums angegeben werden

- **Mündlich weitergegebene Information** - die Vertraulichkeitsstufe vertraulicher Information, die in persönlichen Gesprächen, über Telefon oder andere Kommunikationsarten ausgetauscht wird, muss vor der eigentlichen Information mitgeteilt werden

## Umgang mit klassifizierter Information

Jeder, der Zugang zu sensiblen Informationen hat, muss sich an die Regeln halten, die in der folgenden Tabelle stehen.
Wenn jemand die Regeln bricht oder vertrauliche Infos an unbefugte Personen weitergibt, muss die Geschäftsführung disziplinarische Schritte einleiten.

Falls es zu einem Vorfall im Umgang mit diesen Informationen kommt, muss dieser nach den internen Richtlinien für Datenschutzverletzungen oder Sicherheitsmeldungen geprüft und gegebenenfalls an die zuständigen Stellen gemeldet werden.

Sensible Informationen dürfen die Organisation nur verlassen, wenn eine Genehmigung gemäß der IT-Sicherheitsrichtlinien vorliegt.

| | ***Intern*** | ***Vertraulich**** | ***Streng vertraulich**** |
|---|---|---|---|
| **Papier-Dokumente** | • Nur berechtigte Personen erhalten Zugang<br>• Dokumente dürfen sich nur in Räumen befinden, zu denen die Allgemeinheit keinen Zugang hat<br>• Die Dokumente müssen regelmäßig von Druckern und Faxgeräten entfernt werden | • Dokumente dürfen sich nur in Räumen befinden, zu denen die Allgemeinheit keinen Zugang hat<br>• Dokumente dürfen innerhalb und außerhalb der Organisation nur in einem verschlossenen Umschlag übertragen werden<br>• Die Dokumente müssen umgehend von Druckern und Faxgeräten entfernt werden<br>• Nur der Eigentümer des Dokuments darf es kopieren<br>• Nur der Eigentümer des Dokuments darf es vernichten | • Das Dokument muss in einem verschlossenen Schrank aufbewahrt werden<br>• Das Dokument darf innerhalb und außerhalb der Organisation nur durch eine vertrauenswürdige Person und in einem verschlossenen Umschlag übergeben werden<br>• Versand des Dokuments per Fax ist nicht erlaubt<br>• Das Dokument darf nur ausgedruckt werden, wenn die berechtigte Person sich direkt am Drucker befindet |

| | | | |
|---|---|---|---|
| **Elektronische Dokumente** | • Nur berechtigte Personen erhalten Zugang<br>• Der Zugang zum Informationssystem, in dem das Dokument gespeichert ist, muss durch ein sicheres Passwort geschützt sein<br>• Der Bildschirm, auf dem das Dokument angezeigt wird, muss automatisch nach 15 Minuten Inaktivität gesperrt werden | • Nur Personen mit Zugangsberechtigung für das Dokument dürfen Zugang zu dem Teil des Informations-Systems erhalten, in dem dieses Dokument hinterlegt ist<br>• Beim Austausch von Dateien über Dienste wie FTP, Instant Messaging, etc., müssen sie verschlüsselt sein<br>• Nur der Eigentümer des Dokuments darf es löschen | • Das Dokument muss verschlüsselt gespeichert werden<br>• Das Dokument darf nur auf Servern gespeichert werden, die unter der Leitung der Organisation stehen<br>• Das Dokument darf nicht über Dienste wie FTP, Instant Messaging, etc. ausgetauscht werden |
| **Informations-Systeme** | • Nur berechtigte Personen dürfen Zugang erhalten<br>• Der Zugang zur Information muss durch ein sicheres Passwort geschützt sein<br>• Der Bildschirm muss automatisch nach 15 Minuten Inaktivität gesperrt werden<br>• Das Informationssystem darf sich ausschließlich in Räumen mit überwachtem physikalischem Zugang befinden | • Anwender müssen sich vom Informationssystem abmelden oder dieses sperren, falls sie sich vom Arbeitsplatz vorübergehend oder dauerhaft entfernen<br>• Die Löschung von Daten darf ausschließlich mittels eines Algorithmus erfolgen, der sichere Löschung gewährleistet, dies entfällt bei verschlüsselten Informationssystemen | • Für die Zugangssteuerung zur Information muss ein Authentisierungs-Prozess auf Basis von einem zweiten Faktor eingesetzt werden<br>• Das Informations-System darf ausschließlich auf Servern installiert werden, die unter der Leitung der Organisation stehen<br>• Das Informations-System darf sich ausschließlich in Räumen mit überwachtem physikalischem Zugang befinden, bei denen die Identität von Personen vor dem Zutritt überprüft wird |
| **Elektronische Post** | • Nur berechtigte Personen dürfen Zugang erhalten<br>• Der Empfänger muss die Absenderadresse sorgfältig prüfen<br>• Alle unter „Informationssysteme“ genannten Regeln gelten | • Der Versand von E-Mail außerhalb der Organisation muss verschlüsselt erfolgen | • Alle E-Mails müssen verschlüsselt sein |

| | | | |
|---|---|---|---|
| **Elektronische Datenträger** | • Nur berechtigte Personen dürfen Zugang erhalten<br>• Bei Versand außerhalb der Organisation muss der Datenträger als Einschreiben und/oder Nachverfolgung und/oder mit persönlicher Übergabe versandt werden<br>• Der Datenträger darf nur in Räumen mit überwachtem physikalischem Zugang aufbewahrt werden | • Datenträger und Dateien müssen verschlüsselt und/oder mit einem Password geschützt sein<br>• Datenträger müssen in einem verschlossenen Schrank aufbewahrt werden<br>• Bei Versand außerhalb der Organisation muss der Datenträger als Einschreiben und/oder Nachverfolgung und/oder mit persönlicher Übergabe versandt werden<br>• Nur der Eigentümer des Datenträgers darf diesen löschen oder vernichten | • Datenträger müssen in einem Tresor aufbewahrt werden<br>• Datenträger dürfen innerhalb und außerhalb der Organisation nur durch eine vertrauenswürdige Person und in einem verschlossenen und versiegelten Umschlag übergeben werden |
| **Mündlich weitergegebene Information** | • Nur berechtigte Personen dürfen Zugang zur Information erhalten<br>• Nicht berechtigte Personen dürfen sich nicht im selben Raum aufhalten, während die Information kommuniziert wird | • Die Räumlichkeit muss ein separater und geschlossener Raum sein<br>• Die Unterredung darf nicht aufgezeichnet werden | • Besprechungen, die mit jeglicher Art von Kommunikationsmittel abgehalten werden, müssen verschlüsselt sein<br>• Mitschriften der Gespräche sind nicht erlaubt |

*Maßnahmen verstehen sich kumulativ. Das heißt, Maßnahmen jeglicher Vertraulichkeitsstufe setzen die Umsetzung der Maßnahmen der niedrigeren Vertraulichkeitsstufen voraus. Falls strengere Maßnahmen für eine höhere Vertraulichkeitsstufe vorgeschrieben sind, werden nur diese umgesetzt.