Rollen und Berechtigungen

Worum geht es?

Der Schutz von Vertraulichkeit (Schutz vor unberechtigter Einsichtnahme) und Integrität (Schutz vor unberechtigten Veränderungen) der Informationen und Daten ist durch wirksame Zugriff- bzw. Zugangskontrollen zu gewährleisten. Bestandteil des Identitäts- und Berechtigungsmanagements ist ein wirksames Rollen- und Berechtigungskonzept.

Rechtsgrundlagen

- **§ 28 KomHVO NRW**
- **§ 32 KomHVO NRW**
- **GoBD Rz.103 ff.**
- **DSGVO und DSG NRW**

Erläuterung/Grundinformation

Gemäß § 28 Abs. 5 KomHVO NRW sind bei der Buchführung mit Hilfe automatisierter Datenverarbeitung (DV-Buchführung) die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)zu beachten. Gemäß § 28 Abs. 5 KomHVO NRW muss unter Beachtung der GoBD u.a. sichergestellt sein, dass

nachvollziehbar dokumentiert ist, wer, wann, welche Daten eingegeben oder verändert hat,

in das automatisierte Verfahren nicht unbefugt eingegriffen werden kann,

die gespeicherten Daten nicht unbefugt verändert werden können.

Nach den GoBD sind Kontrollen einzurichten, auszuüben und zu protokollieren. Dazu gehören beispielsweise Zugangs- und Zugriffsberechtigungskontrollen auf Basis entsprechender Zugangs- und Zugriffsberechtigungskonzepte. Die konkrete Ausgestaltung des Kontrollsystems ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems (Rz 100 der GoBD[1]).

§ 32 Abs. 1 KomHVO NRW sieht vor, dass der Hauptverwaltungsbeamte bzw. die Hauptverwaltungsbeamtin nähere Vorschriften über die ordnungsgemäße Erledigung der

[1] Grundsätze ordnungsmäßiger Buchführung, Veröffentlichung des Bundesfinanzministers Berlin, November 2019 https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf?__blob=publicationFile&v=9,

Aufgaben der Finanzbuchhaltung erlässt. Diese örtlichen Vorschriften müssen gemäß § 32 Abs. 2 Ziffer 2.2 KomHVO NRW u.a. mindestens Bestimmungen über den Einsatz von automatisierter Datenverarbeitung in der Finanzbuchhaltung mit Festlegungen über Berechtigungen im Verfahren enthalten.

Die GoBD sehen vor, dass der Nachweis der Durchführung der in dem jeweiligen Verfahren vorgesehenen Kontrollen u.a. durch Verarbeitungsprotokolle sowie durch die Verfahrensdokumentation zu erbringen ist (Rz 60 der GoBD).

Ein anforderungsgerechtes Rollen- und Berechtigungskonzept ist daher ein erforderlicher Bestandteil einer Verfahrensdokumentation.

Auch für die Umsetzung der Anforderungen, die sich aus der DSGVO (Art. 32) und dem DSG NRW (§ 15) bezüglich Vertraulichkeit und Integrität personenbezogener Daten ergeben, ist ein Rollen- und Berechtigungskonzept erforderlich.

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
1	Rollen- und Berechtigungskonzept erforderlich, GoBD Rz 100	Ist ein Rollen- und Berechtigungskonzept vorhanden?	Wenn nein, hat die Verwaltung ein Rollen- und Berechtigungskonzept zu erstellen, dessen konkrete Ausgestaltung der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems entspricht.
2	Passwörter müssen sicher sein, GoBD Rz 103 § 28 Abs. 5 Ziffern 3 und 4 KomHVO IDW RS FAIT 1 Rz 84	Wie erfolgt der Systemzugang (Passwort oder Single-Sign-on)? Verfügt die Organisation über verbindliche Regeln zur Verwendung von Passwörtern? Entsprechen die Regeln den Passwort-Empfehlungen aus dem BSI IT-Grundschutz?	Existieren noch keine organisationsinternen Passwort-Regeln, sollte die Organisation interne Passwort-Vorschriften für das einzuführende Verfahren erstellen. Hierbei empfiehlt es sich, sich an den Empfehlungen des BSI aus dem IT-Grundschutzbaustein „ORP.4 Identitäts- und Berechtigungsmanagement“ [2] zu orientieren. So MÜSSEN z. B. in Abhängigkeit von Einsatzzweck und Schutzbedarf sichere Passwörter geeigneter Qualität gewählt werden. Das Passwort MUSS so komplex sein, dass es nicht leicht zu erraten ist. Das Passwort DARF NICHT zu kompliziert sein, damit der Benutzer in der Lage ist, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden. (ORP.4.A22 Regelung zur Passwortqualität) Konkretisiert werden die Anforderungen in den Umsetzungshinweisen[3] zum genannten Baustein. So sind für ein sicheres Passwort die Länge und die Anzahl der verwendeten Zeichenarten wie Großbuchstaben,

[2] Baustein: ORP.4. Identitäts- und Berechtigungsmanagement: Download unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2022.pdf?__blob=publicationFile&v=3#download=1

[3] Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement: Download unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=4

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
			Kleinbuchstaben, Sonderzeichen und Zahlen in sinnvoller Kombination und in Abhängigkeit des verwendeten Verfahrens zu wählen: • z. B. 20 – 25 Zeichen Länge und zwei genutzte Zeichenarten (weniger komplex, längeres Passwort beziehungsweise Passphrase), • z. B. 8 – 12 Zeichen Länge und vier genutzte Zeichenarten (komplexer, geringere Länge des Passworts), • z. B. bei Mehr-Faktor-Authentisierung 8 Zeichen Länge und drei genutzte Zeichenarten. (ORP.4.M22 Regelung zur Passwortqualität) Bei erhöhtem Schutzbedarf SOLLTE eine sichere Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, zur Authentisierung verwendet werden.
3	Kontrolle der Einhaltung der Ordnungsvorschriften, GoBD Rz 100 IDW PH 9.330.1 Ziffer 4.2	Wie wird sichergestellt, dass die Regelungen zur Passwort-Nutzung eingehalten werden?	Empfehlenswert ist die technische Umsetzung der Passwortregeln (d.h. Passwortlänge, -komplexität und Zyklus Passwortänderung wird systemtechnisch erzwungen) Empfohlene organisatorische Maßnahmen: Dienstanweisung verbietet Weitergabe von Passwörtern an Dritte, Hinweise zur Passwort-Nutzung im Intranet Um die Gefahr versehentlicher Anwendungsfehler zu minimieren, sollten alle MitarbeiterInnen in den korrekten Umgang mit Authentifizierungsverfahren eingewiesen werden.

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
4	Geschäftsanweisung für die Finanzbuchhaltung nach § 32 KomHVO NRW erforderlich	Wird in der Geschäftsanweisung die verantwortliche Stelle bestimmt, von der die Berechtigungen sachgerecht vergeben werden und die deren Einhaltung kontrolliert und überwacht? (siehe § 32 Abs. 1 i.V.m. Abs. 2 Ziffer 2.2 KomHVO) Wenn ja, werden die Regelungen der Geschäftsanweisung umgesetzt?	Beispiel: Die Berechtigungen für den Zugriff auf die DV-Buchführung werden durch die IT-Abteilung vergeben. Die Vergabe einer Berechtigung bedarf der vorherigen Zustimmung der Leitung der Finanzbuchhaltung.
5	IDW PH 9.330.1 Ziffer 4.2 § 32 Abs. 2 Ziffer 2.2 KomHVO § 32 Abs. 2 Ziffer 2.7 KomHVO	Ist definiert und dokumentiert, wer festlegt, welche Berechtigungen im Einzelfall für die Erledigung der jeweiligen Aufgabe erforderlich sind? Dokumentation geben lassen.	Beispiel: Fachabteilungsleitung entscheidet darüber, welche Berechtigungen (Rollendefinition) im IT-Verfahren für die konkrete Aufgabenerledigung erforderlich sind.
6	IDW PH 9.330.1 Ziffer 4.2	Wird die Verknüpfung zwischen der Aufgabe und den dazu erforderlichen Berechtigungen (Rollendefinition) im IT-Verfahren dokumentiert?	Beispiel: Die einer Rolle zugewiesenen Berechtigungen können mittels eines System-Reports tagesaktuell ausgewertet und dokumentiert werden
7	IDW PH 9.330.1 Ziffer 4.2	Ist definiert und dokumentiert, nach welchen Kriterien das Rollen- und Berechtigungskonzept die im Verfahren vorgesehenen Rollen	Beispiele: Fachabteilungsleitung erhält Rolle „Genehmigung“ mit den Berechtigungen „lesen“ und „freigeben“

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
		und Berechtigungen den Beschäftigten konkret zuweist?	Sachbearbeitung erhält Rolle „Bearbeiten“ mit der Berechtigung „Ändern“ für den jeweiligen Zuständigkeitsbereich (Need-to-know-Prinzip). Rechnungsprüfung erhält Rolle “Prüfung“ mit der Berechtigung „lesen“
8	IDW PS 850 Rz 70	Stehen die Berechtigungen mit den Kompetenzen im Einklang?	
9	§ 28 Abs. 5 Nr. 4 KomHVO IDW RS FAIT 1 Rz 84	Wie wird sichergestellt, dass die Berechtigungsvergabe in jedem Einzelfall dem Need-to-know-Prinzip entspricht?	Beispiel: Zu unterscheiden sind: • Keine Berechtigungen (weder erstellen noch lesen oder ändern) • Lesen (Daten nur lesen) • Erstellen (Daten erfassen) • Ändern (Daten erfassen, bearbeiten sowie löschen) Alle Rechte (Vollzugriff auf Daten)
10	GoBD Rz 100	Wie werden bei der Rollenzuordnung Rollenkonflikte berücksichtigt?	Beispiel: Rollenkonflikt: Sachbearbeiter erhält zusätzlich zur Rolle „Bearbeiten“ die Rolle „Genehmigung“ im Vertretungsfall. Mögliche Lösung: Die Vertretungsregelung gilt nur für „fremde“ Fälle. Zur ggfs. nötigen Genehmigung eigener Fälle wird ein weiterer Sachbearbeiter berechtigt (Vier-Augen-Prinzip).
11	§ 28 Abs. 5 Nr. 3 KomHVO	Wie wird sichergestellt, dass nur personalisierte Berechtigungen vergeben werden, so dass jeder Zugriff einer konkreten Person zugeordnet werden kann?	Keine Sammel-/Funktionskennungen für mehrere Nutzer
12	§ 28 Abs. 5 Nr. 4 KomHVO und Need-to-know-Prinzip	Wie werden Veränderungsprozesse im Rollen- und Berechtigungskonzept geregelt?	Beispiele:

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
			Beschäftigte wechseln Stelle, Azubi wechselt Ausbildungsbereich, Aufgaben entfallen oder werden von anderen Beschäftigten wahrgenommen • Die Prozesse Berechtigungsvergabe und -entzug sollten definiert werden.
13	IKS GoBD Rz 100	Wie wird die Rollen- und Berechtigungsvergabe kontrolliert? Werden die Rollendefinitionen regelmäßig aktualisiert?	Beispiel: Fachabteilungsleitung genehmigt schriftlich Zuweisung und Umfang (zeitlich und sachlich) von Rollen und Berechtigungen im IT-Verfahren an Beschäftigte seiner Abteilung (Vier-Augen-Prinzip). Fachabteilungsleitung prüft einmal im Quartal, ob die im IT-Verfahren vergebenen Berechtigungen noch den im Rollen- und Berechtigungskonzept vorgesehenen Rollen entsprechen.
14	Funktionstrennung GoBD Rz 100	Ermöglicht das Verfahren die Zuweisung unbeschränkter Nutzungsrechte, die sowohl administrative als auch sachbearbeitende Zugriffe in allen Bereichen des IT-Verfahrens ermöglichen (Super-User, SAP*)?	Allumfassende und unbeschränkte Nutzungsrechte sollten grundsätzlich nicht vergeben werden.
15	IDW PH 9.330.1 Ziffer 4.4.16	Sieht das Verfahren Berechtigungen für Zugriffe von außen vor (Fernwartung)? Sind Schutzfunktionen für den Einsatz von Fernwartungsfunktionen vorhanden?	Um unkontrollierte Fernzugriffe zu unterbinden, müssen organisatorische Verwaltungsprozesse zum Umgang mit ausgewählten Fernwartungswerkzeugen etabliert werden (BSI-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung)

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
16		Ist geregelt, dass inaktive Benutzerkonten regelmäßig identifiziert und ihre Notwendigkeit kritisch hinterfragt werden?	