Der Bayerische Landesbeauftragte
für den Datenschutz

Dateiablagen als Quelle von Datenpannen

Aktuelle Kurz-Information 65

Stichwörter: Austauschverzeichnisse – Dateiablagen, gemeinsame –Datenpannen, Dateiablagen – SharePoint – Zugriffsberechtigungen | **Stand:** 15. Januar 2026

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Betriebsmittel wie gemeinsame Dateiablagen oder Austauschverzeichnisse sind eine häufige Quelle von Datenpannen, insbesondere in Form der unbeabsichtigten Offenlegung.
- Bei der Arbeit mit sowie der Administration von gemeinsamen Dateiablagen und Austauschverzeichnissen können einige leicht umsetzbare Routinen bereits viele Datenpannen verhindern.

Viele bayerische öffentliche Stellen nutzen neben ihren Fachverfahren auch (zentrale) Dateiablagen in Form von Verzeichnissen auf einem Server. Solche Dateiablagen dienen dem Austausch von Dokumenten, aber auch als Ablageorte für den – gut skalierbaren – Zugriff durch ganz unterschiedliche Nutzergruppen. Auch wenn sich die elektronische Akte (eAkte) zunehmend durchsetzt, werden „einfache“ Dateiablagen noch eine ganze Zeit weit verbreitet bleiben. 1

Oftmals sind zentrale Dateiablagen als eigene Laufwerke mit einem festen Laufwerksbuchstaben eingerichtet, auf die je nach Größe der Dienststelle alle Beschäftigten oder – etwa nach Organisationseinheiten gegliedert – größere oder kleinere Gruppen zugreifen können. Die Verzeichnisnamen in den Laufwerken sind in der Regel so gewählt, dass für die Beschäftigten ersichtlich ist, welche Kategorien von Informationen dort zu erwarten sind. 2

Aus Datenschutzsicht ist eine Dateiablage als Betriebsmittel einzustufen. Ob und welche personenbezogenen Daten in einer Dateiablage gespeichert sind, hängt davon ab, wie sie genutzt wird – das Spektrum kann von kleinen Mengen nahezu belangloser Daten bis zu umfangreichen Beständen besonders schutzbedürftiger Daten reichen. 3

Die vielseitigen Nutzungsmöglichkeiten von Dateiablagen bringen einige Herausforderungen mit sich, die Risiken von Datenpannen eröffnen. Auch wenn Daten in Dateiablagen oft wenig strukturiert gespeichert werden, müssen die Vorgaben des Datenschutzrechts beachtet werden. Zahlreiche beim Landesbeauftragten erstattete Meldungen nach Art. 33 Datenschutz-Grundverordnung (DSGVO) zeigen, dass es bei der Nutzung von Dateiablagen unnötig oft zu Datenschutzpannen kommt. 4

Aus Sicht einer Datenschutzaufsichtsbehörde ist es bedauerlich, dass eine Protokollierung von lesenden Zugriffen oftmals fehlt. In der Regel werden keine Nachweise darüber geführt, wer welche Dateien geöffnet hat; nur schreibende Zugriffe können mit Hilfe von Daten aus dem Betriebssystem rekonstruiert werden, und das auch nur manchmal. Das erschwert die persönliche Zuordnung von „Neugierabrufen“ ganz erheblich. Wie bereits an anderer Stelle dargelegt, ist bei einer solchen Sachlage im Rahmen von Meldungen nach Art. 33 DSGVO regelmäßig anzunehmen, dass ein nicht berechtigter Zugriff stattgefunden hat.[1] 5

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

6 Im Folgenden finden Nutzende und bayerische öffentliche Stellen Hinweise, die Datenpannen vorbeugen helfen.

1. Für Nutzende

Wie kann ich eine Datenpanne verursachen?

7 Stellen Sie sich vor, Sie haben eine Excel-Tabelle mit den dienstlichen Kontaktdaten der Führungskräfte Ihrer Gemeindeverwaltung erstellt und – mit Einwilligung der betroffenen Personen – auch private Telefonnummern aufgenommen, um die Erreichbarkeit in Notfällen sicherzustellen. Die entsprechende Datei stellen Sie in das Verzeichnis „Vorzimmer Bürgermeister", damit alle dort tätigen Dienstkräfte bei Bedarf zugreifen können. Sie nehmen an, dass für das Verzeichnis sonst niemand berechtigt ist. Leider haben Sie nicht bedacht, dass das Verzeichnis mittlerweile zum Datenaustausch mit nachgeordneten Organisationseinheiten genutzt wird, sodass letztlich alle Beschäftigten mit PC im Netzwerk in Ihre Excel-Tabelle Einblick nehmen können. Zugreifen können also neben einigen Beschäftigten, welche die Daten im Rahmen ihrer Aufgaben rechtmäßig zur Kenntnis nehmen dürfen, viele weitere, auf die das nicht zutrifft. Da hier eine nicht passgenaue technisch-organisatorische Maßnahme (Zugriffssteuerung) zu einer Beeinträchtigung der Vertraulichkeit führt, liegt eine Datensicherheitsverletzung (Art. 4 Nr. 12 DSGVO), landläufig formuliert eine Datenpanne vor.

Wie kann ich eine solche Datenpanne vermeiden?

8 Sie sollten sich bewusst sein, dass ein Rückschluss von Verzeichnisnamen auf Zugriffsberechtigungen nicht zuverlässig möglich ist. Prüfen Sie deshalb die Berechtigungen, bevor Sie personenbezogene Daten in einem Verzeichnis ablegen – vor allem, wenn Sie nicht genau wissen, wer zugriffsberechtigt ist. Passen die Berechtigungen nicht oder sind Sie sich unsicher, klären Sie vor Speicherung mit dem IT-Support oder Ihrem Vorgesetzen, welches Verzeichnis geeignet ist. Im Zweifel lassen Sie ein neues Verzeichnis mit den korrekten Berechtigungen anlegen.

Kurz-Anleitung für Nutzende zur Überprüfung von Berechtigungen von Verzeichnissen

9 Berechtigungen von Verzeichnissen[2] können Sie in aktuellen Versionen von Microsoft Windows wie folgt überprüfen:

- Öffnen Sie den Datei-Explorer.
- Klicken Sie mit der rechten Maustaste auf das gewünschte Verzeichnis.
- Wählen Sie „Eigenschaften" aus (Abb. 1).
- Wählen Sie den Reiter „Sicherheit" (Abb. 2).
- Kontrollieren Sie die Zugriffsrechte, indem Sie zunächst überprüfen, welche Gruppen- oder Benutzernamen aufgeführt sind. Durch Markieren des entsprechenden Gruppen-

oder Benutzernamens können Sie im unteren Fenster ablesen, welche Berechtigungen für diese Gruppe oder diesen Benutzer zugelassen sind oder verweigert werden.

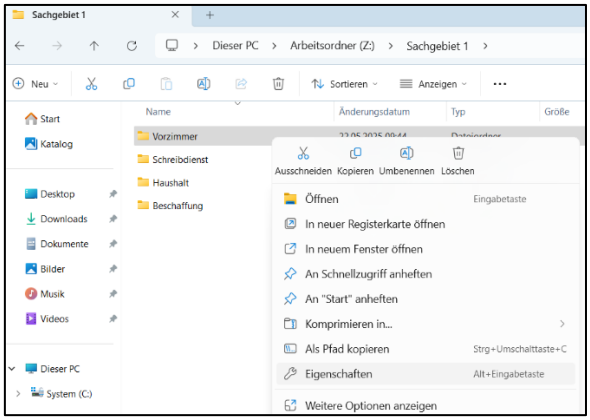

Abb. 1

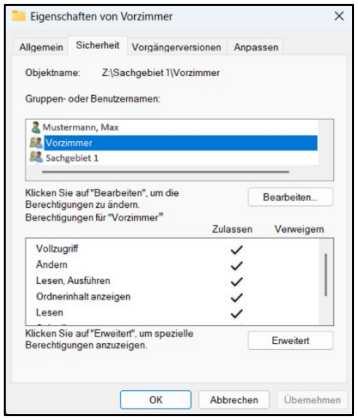

Abb. 2

10

Auch wenn die Berechtigungen aus Ihrer Sicht als passend erscheinen, sollten Sie stets auch bestehende interne Regelungen beachten und im Zweifelsfall nachfragen, für welchen Zweck welches Laufwerk genutzt werden darf.

2. Für Verantwortliche

11

Datenpannen im Zusammenhang mit Dateiablagen können unterschiedliche Ursachen haben. Oft sind unklare Zuständigkeiten, unklare Prozesse oder Unklarheiten bei der Auswahl des korrekten Verzeichnisses Auslöser. Daher ist es sinnvoll, zentrale Festlegungen für die Dateiablage zu treffen und die Beschäftigten bezüglich dieser Festlegungen regelmäßig zu sensibilisieren. Im Folgenden sind Vorschläge für solche Festlegungen aufgelistet, die jedenfalls viele mir in den letzten Jahren gemeldete Datenpannen aus dem Kontext „Dateiablagen“ verhindert hätten – die Beachtung im Alltag natürlich vorausgesetzt:

Prozess zur Verwaltung von Dateiablagen

12

Legen Sie den Prozess für die technische Verwaltung von Dateiablagen fest. Hier sollten mindestens geregelt sein:

- die Stelle, die Verzeichnisse anlegen und löschen sowie Berechtigungen vergeben darf (änderungsberechtigte Stelle, meist der IT-Support),
- die Stellen, die neue Verzeichnisse und Berechtigungsänderungen beantragen dürfen (beauftragende Stellen, beispielsweise Amts- oder Sachgebietsleitungen),
- ein Vier-Augen-Prinzip bei der Berechtigungsvergabe, also die verpflichtende Prüfung der Korrektheit neu vergebener Berechtigungen auch durch die beauftragende Stelle,
- die Dokumentation der Vorgänge „rund um“ Berechtigungen, insbesondere die Dokumentation von Berechtigungsaufträgen sowie deren Erledigung und Überprüfung,

- ein fester Ablauf im Fall des Ausscheidens von Beschäftigten sowie von Versetzungen, Umsetzungen oder anderen Maßnahmen, bei denen sich der Aufgabenkreis ändert, im Hinblick auf bestehende Berechtigungen, etwa eine Verpflichtung der beauftragenden Stelle, relevante Änderungen an die änderungsberechtigte Stelle zu melden,
- die Erstellung und Fortführung einer stets aktuellen und erreichbaren Übersicht für die Beschäftigten, welche Dateiablagen für welche Zwecke vorhanden sind.

Festlegung eines „Kümmerers"

13 Um „Wildwuchs" zu vermeiden, erscheint es zudem als sinnvoll, dass die Organisationseinheit, die inhaltlich die „Hoheit" über ein Verzeichnis hat, insofern als „Kümmerer" fungiert. Einem „Kümmerer" könnten – gegebenenfalls neben den oben Rn. 12 der beauftragenden Stelle (beispielsweise Amts- oder Sachgebietsleitungen) zugewiesenen Aufgaben – insbesondere auch folgende Aufgaben übertragen werden:

- die regelmäßige Prüfung, ob Berechtigungen korrekt gesetzt sind (dies ist insbesondere dann notwendig, wenn Berechtigungen personenbezogen, nicht funktionsbezogen (etwa anhand von gut gepflegten Berechtigungsgruppen) vergeben werden,
- die Pflege der Verzeichnisstruktur (in Bezug auf Unterverzeichnisse),
- die regelmäßige Prüfung, ob Dateien gelöscht werden müssen,
- die Einführung neuer Beschäftigter in die Verzeichnisstruktur und in die Regeln zum Umgang mit den Verzeichnissen,
- im Falle von Umstrukturierungen: die Übergabe der Verantwortlichkeit an eine andere Stelle oder die Löschung des Hauptverzeichnisses.

Regelungen für Austauschverzeichnisse

14 Sollen Verzeichnisse für den Austausch von Dateien innerhalb der öffentlichen Stelle genutzt werden, werden ebenfalls klare Vorgaben benötigt. Hier sollten zumindest festgelegt werden:

- die Zuständigkeit für die Löschung der Dateien (etwa die Person, die das Dokument in das Verzeichnis eingestellt hat),
- die Zuständigkeit für die Prüfung der Sensibilität der Daten (sinnvollerweise ebenfalls die Person, die das Dokument in das Verzeichnis eingestellt hat),
- Maßnahmen, die getroffen werden müssen, wenn die Daten eine hohe Sensibilität aufweisen, wie beispielsweise die Erstellung eines Unterverzeichnisses mit den notwendigen Berechtigungseinschränkungen oder die Vergabe eines Passworts für die Datei oder das Packen der Datei in eine ZIP-Datei mit Passwort,
- eine Löschfrist (beispielsweise spätestens zwei Wochen nach dem Einstellen) und gegebenenfalls die Anforderung an den IT-Support, das Austauschverzeichnis regelmäßig auf

ältere Dateien zu scannen und diese entweder zu löschen oder der einstellenden Person mit dem Ziel der Löschung zu melden.

Ähnliche Problemstellung, anderes System: Microsoft SharePoint

15 Die Nutzung von Microsoft SharePoint als Plattform für die gemeinsame Dokumentenverwaltung bringt ähnliche Herausforderungen und Risiken mit sich wie die Dateiablage auf Dateiservern. Obwohl SharePoint durch seine Funktionen zur Versionierung, Zugriffssteuerung und Zusammenarbeit viele Vorteile bieten kann, besteht auch hier die Gefahr, dass Datenpannen auftreten, insbesondere wenn Berechtigungen nicht sorgfältig verwaltet werden.

16 Bei SharePoint können Berechtigungen auf unterschiedlichen Ebenen (Site-, Bibliotheks- oder Dokumentenebene) vergeben werden. Die Berechtigungsverwaltung ist somit recht komplex. Insbesondere bei SharePoint-Listen oder Dokumentenbibliotheken, die von mehreren Teams genutzt werden, besteht die Gefahr, dass Berechtigungen nicht korrekt gesetzt werden.

17 SharePoint kann im Gegensatz zu „normalen" Dateiablagen auch lesende Zugriffe über sog. Audit-Logs protokollieren. Um Zugriffe nachverfolgen zu können, müssen diese Audit-Logs zum einen korrekt konfiguriert, zum anderen auch, gegebenenfalls regelmäßig, ausgewertet werden. Bei einer Protokollierung muss zuerst insbesondere geprüft werden, ob und gegebenenfalls in welchem Umfang sie aus personal(datenschutz)rechtlicher Perspektive rechtmäßig möglich ist und wer unter welchen Bedingungen dann auf die Protokolldaten zugreifen darf.

18 Die Vielzahl an Funktionen und Einstellungen in SharePoint kann zu einer erhöhten Komplexität bei der Verwaltung führen.

19 **Nutzende** können Datenpannen ähnlich wie oben beschrieben vermeiden: Legen Sie Daten ausschließlich dort ab, wo Sie wissen, dass die Zugriffsberechtigungen korrekt gesetzt und die Ablageorte für den beabsichtigten Zweck auch vorgesehen sind.

20 **Verantwortliche** sollten auch für SharePoint alle oben unter Rn. 11 ff. skizzierten Ratschläge berücksichtigen. Zudem sollte eine korrekte Konfiguration der Audit-Logs sichergestellt werden.

[1] Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Orientierungshilfe, Stand 6/2019, Rn. 18, Internet: https://www.datenschutz-bayern.de/infothek/.

[2] Im Sprachgebrauch von Windows oft auch als „Ordner" bezeichnet.