* 

**Rechte- und Rollenkonzept (Entwurf)**

E-Akte in Strafsachen

Version 0.5 | Stand 09.02.2022



|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Dokumenteninformation** | | | | | | | | | | |
| **Programm** | | | Polizei 20/20 | | | | | | | |
| **Programmleiter** | | | Holger Gadorosi | | | | | | | |
| **Projektleiter/Verantwortlicher** | | | Hendrik Flohr | | | | | | | |
| **Dokumententitel** | | | Rechte- und Rollenkonzept (Entwurf) | | | | | | | |
| **Version** | | | 0.5 | | | | | | | |
| **Erstellt am**  **Erstellt von** | | | 25.08.2021  Zentrales Projektteam (ZPT) | | | | | | | |
| **Zuletzt bearbeitet am**  **Zuletzt bearbeitet von** | | | 09.02.2022  Zentrales Projektteam (ZPT) EAS | | | | | | | |
| **Status** | | | In Bearbeitung  <**X**> | | **Status** | | In Bearbeitung  <**X**> | | **Status** | |
| **Vorprüfung des Dokumentes** | | | | | | | | | | |
| **Fachliche Prüfung** (Fachlichkeit) | | | | | | Vorgelegt < X > | | Freigegeben < > | | |
| **Technische Prüfung** (Technik) | | | | | | Vorgelegt < X > | | Freigegeben < > | | |
| **Methodische Prüfung** (Projektkoordination) | | | | | | Vorgelegt < X > | | Freigegeben < > | | |
| **Freigabe Hauptversion 1.0 durch Freigabeverantwortlichen bzw. zuständiges Gremium** | | | | | | | | | | |
| **Freigegeben am** (TT.MM.JJJJ): | | | | | | | | | | |
| **Freigegeben von** (Nachname, Vorname, OE): | | | | | | | | | | |
| **Unterschrift** (Unterschrift in gescannter Kopie): | | | | | | | | | | |
| **Versionshistorie** | | | | | | | | | | |
| **Version** | **Datum** | **Erstellt durch** | | **Inhaltliche Kurzbeschreibung der Neuerungen** | | | | | |
| 0.1 | 01.11.2021 | Christian Kisch | | Erstellt und im ZPT beraten | | | | | |
| 0.2 | 17.11.2021 | Christian Kisch | | Einarbeitung der Hinweise des BfDI | | | | | |
| 0.3 | 06.01.2022 | ZPT EAS | | Einarbeitung der Teilnehmer-Anmerkungen | | | | | |
| 0.4 | 04.02.2022 | ZPT EAS | | Einarbeitung der Hinweise IAM | | | | | |
| 0.5 | 09.02.2022 | ZPT EAS | | Finalisierung | | | | | |

Inhaltsverzeichnis

[Inhaltsverzeichnis 4](#_Toc88646350)

[Präambel 6](#_Toc88646351)

[1. Geltungsbereich 6](#_Toc88646352)

[2. Gegenstand 6](#_Toc88646353)

[3. Zielsetzung 7](#_Toc88646354)

[4. Grundsätze 8](#_Toc88646355)

[5. Mandantentrennung und Mandantenfähigkeit 9](#_Toc88646356)

[6. Begriffsdefinitionen 10](#_Toc88646357)

[7. Identifikation durch Authentifizierung und Autorisierung 13](#_Toc88646358)

[8. Rollenprofile 14](#_Toc88646359)

[8.1. SuperUser 15](#_Toc88646360)

[8.1.1. Gewährte Entitäten und Aktionsarten 15](#_Toc88646361)

[8.1.2. Gewährte Funktionalitäten 16](#_Toc88646362)

[8.1.3. Besondere Sicherheitsanforderungen 16](#_Toc88646363)

[8.2. Technischer Administrator zentral 17](#_Toc88646364)

[8.2.1. Gewährte Entitäten und Aktionsarten 17](#_Toc88646365)

[8.2.2. Gewährte Funktionalitäten 18](#_Toc88646366)

[8.3. Fachlicher Administrator lokal 19](#_Toc88646367)

[8.3.1. Gewährte Entitäten und Aktionsarten 19](#_Toc88646368)

[8.3.2. Gewährte Funktionalitäten 19](#_Toc88646369)

[8.4. Führungskraft 20](#_Toc88646370)

[8.4.1. Gewährte Entitäten und Aktionsarten 20](#_Toc88646371)

[8.4.2. Gewährte Funktionalitäten 21](#_Toc88646372)

[8.5. Verantwortlicher Sachbearbeiter 22](#_Toc88646373)

[8.5.1. Gewährte Entitäten und Aktionsarten 22](#_Toc88646374)

[8.5.2. Gewährte Funktionalitäten 23](#_Toc88646375)

[8.6. Sachbearbeiter Straf- und Bußgeldakte 24](#_Toc88646376)

[8.7. Beteiligter Sachbearbeiter 25](#_Toc88646377)

[8.7.1. Gewährte Entitäten und Aktionsarten 25](#_Toc88646378)

[8.7.2. Gewährte Funktionsrechte 26](#_Toc88646379)

[8.8. Besondere Rechte für Sachbearbeiter und sonstige Bedienstete (z.B. Geheimschutzermächtigung) sowie für Verfahren (z.B. schützenswerte Inhalte) 27](#_Toc88646380)

[8.9. Bediensteter Elektronische Poststelle/Verwaltung 27](#_Toc88646381)

[8.10. Stellverteter 27](#_Toc88646382)

[8.11. Beteiligter Sachbearbeiter Gastzugang 28](#_Toc88646383)

[8.12. Schulungspersonal 28](#_Toc88646384)

[8.13. Datenschutzbeauftragter 28](#_Toc88646385)

[8.14. Informationssicherheitsbeauftragter 29](#_Toc88646386)

[8.15. IT-Sicherheitsbeauftragter 29](#_Toc88646387)

[8.16. Unvereinbarkeit von Rollenprofilen 30](#_Toc88646388)

[9. Berechtigungsverwaltung 31](#_Toc88646389)

[9.1. Rollen- und Benutzergruppenzuteilung 31](#_Toc88646390)

[9.2. Berechtigungsvergabe 32](#_Toc88646391)

[9.3. Changemanagement 34](#_Toc88646392)

[9.4. Administration der Berechtigungen 34](#_Toc88646393)

[9.5. Dokumentation der Zugriffsrechte 34](#_Toc88646394)

[9.6. Kontrolle der Berechtigungen 35](#_Toc88646395)

[9.7. Kontrolle der Zugriffe und Protokolldateien 36](#_Toc88646396)

[9.8. Benutzung von privilegierten Benutzerkonten 36](#_Toc88646397)

[9.9. Fehlgeschlagene Zugriffsversuche und Berechtigungs-verstöße 37](#_Toc88646398)

[9.10. Entzug von Berechtigungen 37](#_Toc88646399)

[10. Funktionen von e²A und Anpassungsbedarf 37](#_Toc88646400)

[11. Zentrale Erreichbarkeit 38](#_Toc88646401)

# Präambel

Das Projekt Elektronische Akte in Strafsachen (EAS) ist ein Gemeinschaftsprojekt der Polizeien von Bund und Ländern sowie der Zollverwaltung (Teilnehmer) im Rahmen des Programms Polizei 2020. Themenführer des Projektes ist die Bundespolizei. Datenschutzrechtliche Verantwortliche[[1]](#footnote-1) sind die Polizei- und Zollbehörden der Teilnehmer.

Die Verantwortlichen betreiben im Rahmen von Polizei 2020 die Elektronische Akte für das Straf- und Bußgeldverfahren[[2]](#footnote-2) (E-Akten-Lösung). Die Datenverarbeitung erfolgt auf Grundlage der §§ 32 ff. und §§ 496 ff. StPO sowie ggf. § 49d und §§ 110a ff. OWiG. In der E-Akten-Lösung können alle Kategorien personenbezogener Daten verarbeitet werden, die in einem Straf- oder Bußgeldverfahren relevant sind. Dies schließt auch die Verarbeitung besonderer Kategorien personenbezogener Daten und anderer sensibler Daten ein.

Die Verantwortlichen (vgl. § 46 Nr. 7 BDSG) nutzen einen Auftragsverarbeiter (vgl. § 46 Nr. 8 BDSG) für den Betrieb der E-Akten-Lösung. Durch vertragliche Gestaltung und technische Maßnahmen ist sichergestellt, dass der Auftragsverarbeiter selbst keinen Zugriff auf die Daten hat. Die E-Akten-Lösung basiert auf einer elektronischen Akte der Justiz des Landes Nordrhein-Westfalen (e²A), die durch einen Entwickler weiterentwickelt und an die fachlichen Bedürfnisse der Polizei und, soweit noch erforderlich, an die datenschutzrechtlichen Vorgaben technisch angepasst wird. Nach Aufnahme des Wirkbetriebs werden grundlegende Änderungen in der E-Akten-Lösung durch die Verantwortlichen beschlossen und innerhalb des Programms Polizei 2020 umgesetzt.

In der E-Akten-Lösung erfolgen die Benutzerzugriffe auf Grundlage des folgenden Rechte- und Rollenkonzepts. Das Rechte- und Rollenkonzept (insbesondere die Rollenprofile) wird im Rahmen der Weiterentwicklung der E-Akten-Lösung angepasst.

# Geltungsbereich

Das Rechte- und Rollenkonzept gilt für den Betrieb der Elektronische Akte in Straf- und Bußgeldsachen (E-Akten-Lösung). Die Vorgaben des Rechte- und Rollenkonzepts sind für alle Bediensteten bzw. Mitarbeiter der Verantwortlichen und Auftragsverarbeiter, die die E-Akten-Lösung nutzen (Anwendung und Administration), verbindlich.

# Gegenstand

Das Dokument beschreibt das Rechte- und Rollenkonzept der E-Akten-Lösung, das der Berechtigungsvergabe, der Berechtigungsänderung und dem Berechtigungsentzug der Bediensteten bzw. Mitarbeiter der Verantwortlichen und der Auftragsverarbeiter zugrunde liegt. Begriffsbestimmungen sind der **Anlage 1** zu entnehmen.

Im Rechte- und Rollenkonzept werden die Berechtigungen zur Nutzung der zentralen E-Akten-Lösung beschrieben und den jeweiligen Funktionalitäten zugeordnet. Hierbei wird zwischen Administratoren und Anwendern unterschieden. Die Festlegungen orientieren sich an den Rollen, Funktionalitätsrechten und Entitätsberechtigungen, die innerhalb der Software den einzelnen Anwendern zugewiesen werden können.

Die Nutzung beinhaltet

* das Erstellen, Verändern, Löschen und Verwalten von Verfahren, Akten/Aktenkopien, Ordnern, Teilakten/Teilaktenkopien, Dokumenten und Metadaten,
* den Umfang des Zugriffs auf Verfahren, Akten/Aktenkopien innerhalb der eigenen Dienststelle,
* den Umfang des Zugriffs auf Verfahren, Akten/Aktenkopien bei temporärer dienstellen-/mandantenübergreifender Freigabe
* die Berechtigung zum Übermitteln von Akten/Aktenkopien, Teilakten/Teilaktenkopien, Dokumenten und Metadaten und
* das Erstellen und Verwalten einer Dienststellenstruktur.

Zusätzlich werden im Rechte- und Rollenkonzept die Voraussetzungen zur Erteilung der Berechtigungen definiert sowie der Prozess und das Verfahren zur Genehmigung und Vergabe von Berechtigungen beschrieben. Darüber hinaus wird eine Musterliste zur Verfügung gestellt, in der die vergebenen Rollen und Funktionalitäten den jeweiligen Benutzern zugeordnet werden können.

Das Rechte- und Rollenkonzept unterscheidet zwischen den Berechtigungen auf Funktionalitäten, die in Form von Rollen vergeben werden, und der Berechtigung auf Daten (z.B. Metadaten, Protokollierungsdaten, Anwenderverwaltungsdaten), die durch die Zugehörigkeit zu einer Dienststelle oder einer Gruppe definiert sind. Ein Benutzer kann, unter Berücksichtigung der Rollentrennung, mehreren Benutzergruppen zugeordnet sein.

Die folgenden Risiken sind für das Identitäts- und Berechtigungsmanagement von Bedeutung:

* Ausspähen von Informationen (Spionage),
* Diebstahl von Dokumenten,
* Fehlplanung oder fehlende Anpassung,
* Manipulation von Informationen,
* unbefugtes Eindringen in IT-Systeme,
* Ausfall von Geräten oder Systemen,
* Verstoß gegen Gesetze oder Regelungen,
* unberechtigte Nutzung oder Administration von Geräten und Systemen,
* fehlerhafte Nutzung oder Administration von Geräten und Systemen,
* Missbrauch von Berechtigungen,
* Identitätsdiebstahl,
* Abstreiten von Handlungen,
* Integritätsverlust schützenswerter Informationen.

# Zielsetzung

Ziel dieses Rechte- und Rollenkonzepts ist die Kontrolle des geregelten Zugriffs auf Informationen. Befugten Nutzern soll der Zugang und Zugriff zu Informationen in der E-Akten-Lösung gesichert ermöglicht und unbefugter Zugang und Zugriff unterbunden werden.

Das Rechte- und Rollenkonzept sorgt für eine konsistente, einheitliche und transparente Vergabe und den rechtzeitigen Entzug von Berechtigungen auf Ressourcen (Organisation).

Das Rechte- und Rollenkonzept sorgt für die Umsetzung der Vorgaben der Informationssicherheit und des Datenschutzes, aber auch einer konformen Leitung (Compliance).

Das Rechte- und Rollenkonzept erteilt zum richtigen Zeitpunkt den richtigen Benutzern die richtigen Zugriffsrechte auf die richtigen Ressourcen (Datenverfügbarkeit).

# Das Rechte- und Rollenkonzept liefert die Transparenz für die Kontrolle der Berechtigungen, sowohl konzeptionell als auch in der praktischen Anwendung (Kontrolle).Grundsätze

Dem Rechte- und Rollenkonzept liegen die nachfolgenden Grundsätze zugrunde:

Die korrekte Berechtigungsvergabe setzt eine verlässliche Identifikation der Benutzer voraus. Alle Benutzer erhalten ihre Anmeldedaten nach klaren Regeln und Sicherheitsvorgaben. Die Art des Identifikationsverfahrens richtet sich risikobasiert nach dem Schutzbedarf der Daten sowie des Zugriffsvektors. Dies und die nachvollziehbare Datenbearbeitung implizieren auch, dass keine nicht personalisierten Benutzer-Accounts vorhanden sein dürfen. Ausnahme bilden sogenannte technische Service-Accounts, die einzelne privilegierte Dienste ausführen und die ausschließlich von Systemen und nicht von Personen verwendet werden, sowie ggf. das Schulungssystem, in dem keine Echtdaten zulässig sind.

Für bestimmte Funktionsprofile werden bestimmte Kompetenzen vorausgesetzt, damit der Bedienstete die E-Akten-Lösung anwenden bzw. administrieren kann. Der Berechtigungsvergabe durch die Verantwortlichen der Teilnehmer ist die Prüfung der Fachkompetenznachweise (z. B. Schulungsnachweis) für die Funktion voranzustellen.

Benutzer werden mit den Berechtigungen ausgestattet, die sie für die Erfüllung ihrer dienstlichen Aufgaben benötigen. Leitlinie ist somit das Prinzip der geringsten Berechtigung: So wenig wie möglich, so viel wie zwingend erforderlich. Sollten sich für ihre Aufgaben weitergehende Anforderungen ergeben, werden die Berechtigungen nach Genehmigung durch die verantwortliche Stelle (z. B. Vorgesetzter, Dezernatsleiter oder Abteilungsleiter) erweitert.

Bei der Rollenzuteilung müssen die Vorgaben der Aufgabentrennung (Segregation of Duty) als Grundlage berücksichtigt werden. So dürfen beispielsweise Datenbank-Administratoren nicht an sich selber System-Administratorenrechte vergeben.

Es müssen klare, einheitliche und nachvollziehbare Prozesse zur Beantragung, Prüfung, Bewilligung, Erteilung, Sperrung und Löschung von Rollen und Berechtigungen bestehen. Allgemeine Rahmenvorgaben der Berechtigungsverwaltung werden im Rechte- und Rollenkonzept getroffen. Im Übrigen wird dies durch die Verantwortlichen der Teilnehmer festgelegt.

Das 4-Augen-Prinzip wird auf sensible Rollen oder Funktionalitäten beschränkt. Es wird im Rechte- und Rollenkonzept für die Teilnehmer oder weitergehend durch den Verantwortlichen eines Teilnehmers für dessen Organisationseinheit festgelegt. . Zur Vermeidung von Interessenkollisionen im Rahmen des 4-Augen-Prinzips ist es erforderlich, dass die beiden Bediensteten bzw. Mitarbeiter voneinander persönlich und organisatorisch getrennt sind. Beide müssen über ein ausreichendes Fachwissen verfügen, damit die Kontrollfunktion ausgeübt wird. Die Durchführung des 4-Augen-Prinzips ist zu dokumentieren. Sofern dies möglich und praktikabel ist, wird die Einhaltung des 4-Augen-Prinzips technisch sichergestellt. In festgelegten Ausnahmesituationen kann von der Einhaltung des 4-Augen-Prinzips abgewichen werden, wenn dies erforderlich ist.

Das Rechte- und Rollenkonzept soll sich an den Berechtigungen der Vorgangsbearbeitungs- und Bußgeldsysteme orientieren, um eine aufwendigere Benutzerverwaltung zu vermeiden. Jeder Benutzer nimmt die ihm festgelegten Aufgaben wahr. Diese Aufgabenwahrnehmung wird über die vordefinierten Rollen abgebildet. Somit werden dem Benutzer funktionale Möglichkeiten zum Arbeiten in der E-Akten-Lösung eingeräumt.

Prämisse ist, dass jeder Benutzer mindestens einer Dienststelle zugeordnet sein muss. Wechselt ein Nutzer die Dienststelle oder nimmt er eine anderweitige oder eine zusätzliche neue Aufgabe wahr, so sind die Berechtigungen anzupassen oder sie werden gelöscht und neue Berechtigungen vergeben. Diese Änderungen müssen im IAM des Teilnehmers erfolgen und an das IAM des Programms Polizei 20/20 übermittelt werden.

Änderungen von Berechtigungen bzw. Benutzerstammdaten müssen unverzüglich ausgeführt werden, um die Aktualität zu gewährleisten.

Personenbezogene Daten und Dokumente dürfen nur verarbeitet werden, wenn dafür eine gesetzliche Grundlage besteht oder die Bearbeitung für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist (Rechtmäßigkeit).

Bei allen Verarbeitungen von personenbezogenen Daten und Dokumenten muss der Grundsatz der Verhältnismäßigkeit beachtet werden. Dieser Grundsatz verlangt, dass nur diejenigen Daten und Dokumente verarbeitet werden, welche für die Erfüllung der gesetzlichen Aufgabe erforderlich sind (Need-to-Know-Prinzip). Dies ist im Rollen- und Berechtigungs-Konzept abzubilden.

Die Grundsätze der Vollständigkeit, Wahrheit, Klarheit, Auffindbarkeit und Manipulationssicherheit der Akte/Aktenkopie werden gewährleistet.

Der Verantwortliche, welcher personenbezogene Daten und Dokumente zur Erfüllung seiner Aufgaben verarbeitet, ist für den Umgang mit diesen Daten und Dokumenten verantwortlich (Informationseigner). Er hat dafür zu sorgen, dass die Verarbeitung ausschließlich rechtmäßig erfolgt. Ihm obliegt zudem der Schutz der Daten durch angemessene organisatorische und technische Maßnahmen. Eine organisatorische Maßnahme stellt beispielsweise die klare Definition von Funktionalitäten und deren Abgrenzung voneinander dar. Die Implementierung einer Zugriffsbeschränkung auf benötigte Daten und Dokumente basierend auf den vergebenen Berechtigungen ist demgegenüber eine technische Maßnahme.

# Mandantentrennung und Mandantenfähigkeit

Die Verantwortlichen der Teilnehmer am Projekt EAS werden als Mandanten die E-Akten-Lösung nutzen. Es muss unter anderem die hinreichende Abgeschlossenheit der jeweiligen Mandanten in der Software und auf einer gemeinsamen Infrastruktur sichergestellt werden.

Für die Zugriffsberechtigungen, Verarbeitungsfunktionen und Konfigurationseinstellungen bedeutet dies, dass sie für jeden Mandanten eigenständig festzulegen sind. Dies umfasst das Anlegen von mandantenspezifischen Benutzerkennungen und eigenständigen Rollen sowie getrennte auf der Ebene des jeweiligen Mandanten abgeschlossene Systeme zur Berechtigungsvergabe. Es muss der Zugang zu mandantenspezifischen Einträgen und zu Einträgen der mandantenübergreifenden Verwaltung gewährleistet werden.

Durch das Rechte- und Rollenkonzept wird sichergestellt, dass zwischen den Mandanten grundsätzlich keine willkürliche Aufhebung rechtlich gebotener Grenzen des Zugriffs auf Verfahren, Ordner, Daten, Dokumente, Akten/Aktenkopien, Dateisysteme und Prozesse durch hierarchisch übergeordnete Rollen und kein Unterlaufen der Zugriffsgrenzen auf der Ebene der verwendeten Informations- und Kommunikationstechniken bzw. durch die eingebundenen Auftragsverarbeiter erfolgt. Die Zugriffskontrolle zu IT-Systemen, Anwendungen, Verfahren, Ordner, Akten/Aktenkopien, Dokumente und Daten wird im Rahmen des Identitätsmanagements, einschließlich der Authentifizierung und Autorisierung, klar geregelt.

Im Übrigen wird auf das Mandantentrennungskonzept verwiesen.

# Identifikation durch Authentifizierung und Autorisierung

Für die Identifikation der Benutzer in der E-Akten-Lösung wird auf das Active Directory und die Identifizierungsinformationen der jeweiligen Verantwortlichen zurückgegriffen. Die Authentifizierungsdaten werden verschlüsselt übermittelt und gespeichert. Jedem Benutzer ist eine eigene Benutzerkennung mit Kennwort zugeordnet. Es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten. Der Anmeldevorgang eines Benutzers muss die nachfolgenden Mindestanforderungen erfüllen:

* Authentifizierung des Benutzers erfolgt durch Eingabe von Benutzernamen und Kennwort.
* Benutzername und Kennwort werden gemäß den Behördenrichtlinien erstellt.
* Die Authentifizierung muss so gestaltet sein, dass ein Benutzer eindeutig identifiziert und einem Benutzerkonto zugeordnet werden kann.
* Die Authentifizierung muss vor jeder anderen Interaktion zwischen System und Benutzer erfolgen.
* Die Authentifizierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf Zugriff haben.
* Die Autorisierung auf Dateien, Verzeichnisse oder Programme erfolgt anhand der Rollenzuordnung nach erfolgreicher Authentifizierung.

In Abhängigkeit von der technischen Umsetzung werden die erforderlichen Informationen über das bereitgestellte IAM (Identity- and Access Management) zur Verfügung gestellt. Das bereitgestellte IAM ist für den Authentifizierungs- und Autorisierungsvorgangs eines Benutzers verantwortlich. Mit Authentifizierung und Autorisierung auf die E-Akten-Lösung endet die Verantwortung des IAM-Dienstes.

Authentifizierung bedeutet, eine Identität durch identitätsgebundene Informationen zu prüfen und zu bestätigen. Diese kann mittels dreier Objekte durchgeführt werden: (1) Preisgabe von Wissen (Benutzerkennung und Passwort), (2) Verwendung eines Besitzes (Token), Nutzung des eigenen Subjekts (z. B. Biometrie-Scan).

Bevor der Benutzer die E-Akten-Lösung nutzen kann, muss er sich mit seiner Benutzerkennung und seinem Passwort an seinem Computer anmelden. Der Zugriff auf die E-Akten-Lösung erfolgt über ein zentrales IAM.

Nachdem die Identität des Benutzers festgestellt wurde, erfolgt die Autorisierung. Hierbei handelt es sich um eine Berechtigung bzw. ausdrückliche Zulassung, durch die festgelegt wird, was für wen in der E-Akten-Lösung erlaubt ist und auf welche Ressourcen zugegriffen werden darf. Die Identität bekommt bestimmte Rechte zugewiesen, auf deren Grundlage sie bestimmte Aktionen in der E-Akten-Lösung durchführen darf (ObjektID, Benutzer, Dataset, Zugriffserlaubnis). Für die E-Akten-Lösung erfolgt eine rollenbasierte Zugriffskontrolle, wobei es auch möglich ist bestimmte Ressourcen (z. B. sensible Dokumente oder eingriffsintensive Funktionen der E-Akten-Lösung) einzuschränken. Einschränkungen können auch durch eine regelbasierte Zugriffskontrolle (z. B. beim maschinellen Abgleich personenbezogener Daten mit einzelnen, zuvor individualisierten elektronischen Akten oder elektronischen Aktenkopien) oder Schnittstellen mit eingeschränkten Rechten (z. B. bei der Übermittlung von Dokumenten) erfolgen.

Erst nach dem Authentifizierungs- und Autorisierungsvorgang kann der Anwender auf die Fachanwendung und die ihm nach Rechte- und Rollenkonzept zugewiesenen Funktionen und Inhalte zugreifen.

# Rollenprofile

Werden Benutzerberechtigungen individuell und direkt auf die IT-Ressourcen vergeben, führt dies in kurzer Zeit zu Unübersichtlichkeit und einem großen administrativen Aufwand. Sollten gar verschiedene Administratoren auf verschiedenen Systemen und Ressourcen ohne klare Prozesse die Zugriffsrechte vergeben können, ist die Nachvollziehbarkeit nicht mehr gewährleistet. Die Kontrollfrage, wer hat wo, wann, und warum welche Zugriffsrechte, ist dann kaum zu beantworten. Aus diesem Grund wird in der E-Akten-Lösung ein rollenbasiertes Rechte- und Rollenkonzept umgesetzt (RBAC).

Das Rechte- und Rollenkonzept knüpft an die gesetzlichen Aufgaben (Strafverfolgung und Verfolgung von Ordnungswidrigkeiten) und die Geschäftsprozesse der jeweiligen öffentlichen Stelle an. Bei diesem Ansatz werden den Benutzern ihre (Geschäfts-)Rollen zugeteilt. Die Rollen ihrerseits enthalten die Berechtigungen auf IT-Ressourcen der E-Akten-Lösung. Die Rollen bilden so die Schnittstelle zwischen Benutzern und Ressourcen. Verschiedene Rollen können zu Benutzergruppen zusammengefasst werden. Diese konzeptionellen Vorgaben müssen auf der Technikebene umgesetzt und im Rahmen der Berechtigungsmanagements kontrolliert werden.

Eine Person kann mehrere Rollen besitzen bzw. mehreren Benutzergruppen angehören, basierend auf ihren Aufgaben, Kompetenzen und Funktionalitäten, die aus den Geschäftsprozessen abgeleitet sind.

Die Rollen müssen einen Feinheitsgrad (Granularität) aufweisen, der eine Umsetzung des Verhältnismäßigkeitsprinzips „Need-to-Know“ ermöglicht. Eine Rolle soll nur die Berechtigungen enthalten, welche für die Erfüllung einer Aufgabe tatsächlich notwendig sind. Zur Erfüllung des mehrschichtigen Aufgabengebietes werden in der E-Akten-Lösung mehrere Rollen vergeben und mit verschiedenen Funktionalitäten verknüpft. Weiterhin wird die Aktionsart einer Rolle bestimmt (vgl. Nummer 6 Buchstabe h).

Benutzer können in Benutzergruppen zusammengefasst werden. Dadurch können für mehrere Benutzer gleichzeitig Rollen verwaltet werden. Den Benutzergruppen sind Rollen zugewiesen. Ein Benutzer, der einer Benutzergruppen zugeordnet ist, erhält automatisch alle Rollen dieser Gruppe.

Abhängig von der Aufgabe und der Organisationseinheit eines Verantwortlichen kann es sinnvoll sein, die Berechtigungen auf Informationsobjekten basierend, auf der Organisationszugehörigkeit des Benutzers, des aktuellen Prozessschrittes (Workflow) und/oder anderer Kriterien automatisiert und dynamisch zu steuern.

In der E-Akten-Lösung gibt es die nachfolgenden Rollenprofile. Das Rechte- und Rollenkonzept kann jederzeit um weitere Rollenprofile bzw. die bestehenden Rollenprofile können ergänzt werden. Die Funktionen des SuperUser und des technischen Administrators zentral werden im Betriebskonzept beschrieben.







## Lokaler Administrator

Die Aufgabe des lokalen Administrators wird jeweils von Bediensteten innerhalb der Verantwortlichen/ Teilnehmer übernommen. Er weist unter anderem den jeweiligen Benutzern ihre entsprechenden Rollen zu. Im Falle von Personalmaßnahmen und Aufgabenwechsel, die Auswirkungen auf die Berechtigungen haben können, wird der lokale Administrator – gemäß den Vorgaben innerhalb der Verantwortlichen – durch die personalführende Stelle oder die Dienst- oder Fachvorgesetzten informiert und nimmt die erforderlichen Anpassungen vor. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 2** zu entnehmen.







## Führungskraft

Eine Führungskraft kann, soweit sie dafür berechtigt wird, aufgrund ihrer Dienst- und Fachaufsicht Einsicht in die Verfahren nehmen, die im Bereich der eigenen Organisationseinheit/en liegen. Darüber hinaus kann eine Führungskraft die Qualitätssicherung/Freigabe von Verfahren vornehmen und ggf. anschließend die Abgabe von Verfahren veranlassen. Soll eine Führungskraft auch als Sachbearbeiter tätig werden, muss ihr zusätzlich die Rolle eines Sachbearbeiters zugewiesen werden. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 3** zu entnehmen.







## Führungskraft mit eingeschränkten Befugnissen

Es gelten die Ausführungen zur Führungskraft entsprechend. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 4** zu entnehmen.

## Verantwortlicher Sachbearbeiter

Den verantwortlichen Sachbearbeitern eines Verfahrens werden weitgehende Berechtigungen eingeräumt. Ihnen sollen grundsätzlich alle Bearbeitungsfunktionalitäten sowie weitere Rechte (u.a. Berechtigung weiterer Sachbearbeiter) zur Verfügung stehen. Bei komplexen Ermittlungen (Mordkommission, BAO usw.) sollte diese Rolle nur dem Leiter der Ermittlungen und/oder sonstigen besonders beauftragten Personen zugewiesen werden. Diese haben somit das alleinige Recht der Erfassung, Änderung, Löschung und Strukturierung des Verfahrens bzw. innerhalb der Verfahrens. Alle übrigen Sachbearbeiter erhalten dann die Rolle „beteiligter Sachbearbeiter“. Dadurch wird sichergestellt, dass nur der Ermittlungsführer über Verfahrens- und Aktenaufbau sowie Akteninhalt bestimmen kann. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 5** zu entnehmen.



## Sachbearbeiter Straf- und Bußgeldakte

Für den Sachbearbeiter Straf- und Bußgeldakte gelten die Rollenbeschreibung, Funktionalitäten, Entitäten und Aktionsarten der Rolle „verantwortlicher Sachbearbeiter“. Zusätzlich zu der Rolle „verantwortlicher Sachbearbeiter“ werden bei den Strafakten des Zolls und den Bußgeldakten Funktionen einer funktionalen Staatsanwaltschaft bzw. einer Bußgeldbehörde übernommen. Aufgrund dessen sind zu der o.a. Rolle weitere Funktionalitäten durch die jeweiligen Sachbearbeiter wahrzunehmen. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 6** zu entnehmen.

## Beteiligter Sachbearbeiter

Der beteiligte Sachbearbeiter eines Verfahrens unterstützt den verantwortlichen Sachbearbeiter, indem er z.B. eigene Erkenntnisse, die er ermittelt hat bzw. die ihm zur Kenntnis gebracht wurden, hinzufügt. Das Ablegen ist für den beteiligten Sachbearbeiter lediglich im Ordner „Entwürfe“, „Eingang“ und „Ablage“ möglich. Die Verantwortung für das Verfahren und somit die Strukturierung obliegt dem verantwortlichen Sachbearbeiter. Auf den zugewiesenen Ordner „Akte“ und die dazu ggf. eingerichteten Unterordner besitzt der beteiligte Sachbearbeiter ausschließlich lesenden Zugriff. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 7** zu entnehmen.



## 

## Bediensteter Elektronische Poststelle/Verwaltung

Die Rolle Bediensteter Elektronische Poststelle/Verwaltung dient der Steuerung von Posteingängen über das zentrale Teilnehmerpostfach. Sie beinhaltet die manuelle Zuordnung und Weiterleitung von Eingängen an Benutzergruppen/Organisationseinheiten und ggf. an Sachbearbeiter. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 8** zu entnehmen.

## Bediensteter Geschäftsstelle

Unter anderem beim Zoll sind Geschäftsstellen in einigen Organisationseinheiten eingerichtet, denen zur Aktenbearbeitung bestimmte Aufgaben zugewiesen sind (Eingangsbearbeitung, Einholen von Auskünften, ggf. Zahlungsabwicklung). Der Bedienstete Geschäftsstelle erhält die Befugnis zum Anlegen von Akten und zur Zuweisung der verantwortlichen Sachbearbeiter sowie einen schreibenden Zugriff auf die Akte in Form der Erstellung und Ablage von Dokumenten. Dies hat ausschließlich innerhalb der Ordner „Entwürfe“, „Eingang“ und „Ablage“ zu erfolgen. Auf die Ordner „Akte“ und die dazu ggf. eingerichteten Unterordner besitzt der Rolleninhaber lesenden Zugriff. Dem Bediensteten Geschäftsstelle werden zu den ihm zugewiesenen Ressourcen auch die Berechtigungen zum Suchen, Ausführen und Abbrechen erteilt, soweit dies für die Aufgabenerfüllung erforderlich ist. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 9** zu entnehmen.

## Bediensteter Registratur

Abgeschlossene Bußgeldakten und Strafakten (Zoll) müssen nach Ablauf der Aufbewahrungsfrist dem zuständigen Archiv zur Übernahme angeboten werden (z.B. §§ 5, 7 BArchG). Hierzu erstellt die zuständige Stelle des Teilnehmers ein Verzeichnis mit festgelegten Angaben zu den anzubietenden Akten (z.B. Aktenzeichen, Betreff, Zeitraum der Bearbeitung der Akte) und übermittelt dieses an das zuständige Archiv. Ggf. gewährt die zuständige Stelle des Teilnehmers Mitarbeitern des Archives Einsicht in die angebotenen Akten, damit diese über die Archivwürdigkeit entscheiden können. Auf entsprechende Mitteilung des Archives übergibt die zuständige Stelle des Teilnehmers die angeforderten Akten an das Archiv.

Zur Erfüllung dieser Aufgaben benötigt der Bedienstete der Registratur Zugriff auf die Metadaten zu abgeschlossenen Bußgeldakten und Strafakten Zoll sowie das Recht zur Übermittlung dieser Akten an das Archiv. Ein Leserecht in den Akten ist damit nicht verbunden. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 10** zu entnehmen.

## Sachbearbeiter mit Lese-Recht

Mit dieser Rolle soll Sachbearbeitern das Lesen von Verfahrensinhalten ermöglicht werden. Dies kommt insbesondere für Sachbearbeiter in Betracht, die Erkenntnisse aus dem Verfahren für ihre Arbeit benötigen.

Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 11** zu entnehmen.

## Rechts- und Fachaufsicht

Zur Ausübung der Rechts- und Fachaufsicht über die Tätigkeiten nachgeordneter Behörden im Ermittlungs-, Straf- und Bußgeldverfahren ist ein lesender Zugriff auf die Verfahren der nachgeordneten Behörden sowie auf die dazugehörigen statistischen Daten erforderlich. Diese Rechts- und Fachaufsicht wird z.B. im Rahmen einer Geschäftsprüfung ausgeübt. Eine solche Geschäftsprüfung wird in der Regel anhand einer Auswertung der statistischen Daten der von den nachgeordneten Dienststellen bearbeiteten Verfahren vorbereitet. Die Geschäftsprüfung selbst erfolgt über einen lesenden Zugriff auf die Verfahren. Darüber hinaus wird die Bearbeitung einzelner Verfahren der nachgeordneten Behörden fachlich und rechtlich unterstützt (z.B. Verfahren mit bundesweiter Bedeutung wegen der Auslegung rechtlicher Vorschriften). Der lesende Zugriff auf die Verfahren muss im Einzelfall begründet werden. Der Zugriff auf die Verfahren und die Begründung hierfür werden protokolliert. Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 12** zu entnehmen.

## Datenschutzbeauftragter

Der behördliche Datenschutzbeauftragte nimmt insbesondere die folgenden Aufgaben, bei denen ein Datenzugriff erforderlich ist, in Bezug auf die E-Akten-Lösung wahr:

* Überprüfung der Rechtmäßigkeit der Datenverarbeitung,
* Einsichtnahme und Auswertung von Protokolldaten (grundsätzlich unter Einhaltung des 4-Augen-Prinzipes, ausnahmsweise nicht bei dringenden Datenschutz- oder IT-Sicherheitsvorfällen) zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung sowie zur Beratung bei der Eigenüberwachung und der Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten,
* Unterrichtung und Beratung der Behördenleitung und der Bediensteten bzw. Mitarbeiter,
* Wahrnehmung der Kontrollkompetenz in Bezug auf die Anwendung und das IT-System,
* Überprüfungen und Durchführung von Datenschutzaudits,
* Überprüfung des Datenschutzkonzeptes und der Datenschutzmaßnahmen auf deren Wirksamkeit und Nachvollziehbarkeit,
* Überwachung der Einhaltung der Vorgaben des BDSG und etwaiger spezialgesetzlicher Vorschriften (vgl. StPO und OWiG),
* Überwachung der Einhaltung des Grundsatzes der Datenminimierung und der Datensparsamkeit in Bezug auf personenbezogene Daten,
* Überwachung der Einhaltung der technischen und organisatorischen Maßnahmen nach Stand der Technik,
* Einbindung in die Zusammenarbeit mit den und der Prüfung durch die Aufsichtsbehörden oder Auftraggeber, insbesondere bei einer notwendigen Anhörung der Aufsichtsbehörden,
* Führung eines Meldesystems für Datenschutzereignisse und Hinwirken auf korrektive Maßnahmen,
* Unterstützung bei Auskunftsersuchen betroffener Personen oder bei der Benachrichtigungspflicht.

Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 13** zu entnehmen.

## Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte nimmt insbesondere die folgenden Aufgaben, bei denen ein Datenzugriff erforderlich ist, in Bezug auf die E-Akten-Lösung wahr:

* Berichterstattung direkt an die Behörden- bzw. Unternehmensleitung,
* Wahrnehmung der Kontrollkompetenz der Behörde,
* Einbindung in die Durchführung des IT-Projektes,
* Durchführung von Risikoanalysen für das IT-System,
* Bewertung und Kategorisierung des IT-Systems (Applikationen, Services, Server, Netzwerk, Infrastruktur und andere) nach Kritikalität und angemessenem Schutz,
* Überprüfung des IT-Projektes und IT-Systems auf IT-Sicherheit vor Inbetriebnahme in Bezug auf sensible und personenbezogene Daten,
* Überprüfung der Informations- und IT-Sicherheitskonzepte und -maßnahmen auf deren Wirksamkeit und Nachvollziehbarkeit,
* Sicherstellung der physischen, umgebungsbezogenen und technischen Sicherheit,
* Sicherstellung von Verfahren und Maßnahmen zur IT-Sicherheit innerhalb der IT-Betriebsorganisation und Überwachung von deren Einhaltung,
* technische Überwachung der Einhaltung der korrekten Berechtigungsvergaben in IT-Systemen und Applikationen
* Überprüfung der IT-Sicherheitskonzepte auf deren Wirksamkeit,
* Durchführung von Sicherheitsaudits und Schwachstellenprüfungen zur Informationssicherheit,
* Einsichtnahme und Auswertung von Protokolldaten (grundsätzlich unter Einhaltung des 4-Augen-Prinzipes, ausnahmsweise nicht bei dringenden Datenschutz- oder IT-Sicherheitsvorfällen) zur Beratung bei der Eigenüberwachung und der Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten,
* Zusammenarbeit mit Behörden bei Computerstraftaten,
* Führung eines Meldesystems für Informations- und IT-Sicherheitsereignisse und Hinwirken auf korrektive Maßnahmen,
* Überwachung der Einhaltung der Kennzeichnungs- und Klassifizierungsrichtlinien (Need-to-Know-Prinzip),
* Unterstützung bei Prüfungen durch Dritte (z. B. Ermittlungsbehörden, Bundes- und Landesbehörden, unabhängigen Auditoren).

Die gewährten Entitäten, Aktionsarten und Funktionalitäten sind der **Anlage 14** zu entnehmen.

## 

# Berechtigungsverwaltung

## Rollen- und Benutzergruppenzuteilung

Jedem Benutzer wird durch die jeweils zuständige Organisationseinheit eines Teilnehmers anhand seines ihm zugewiesenen Funktions- bzw. Stellenprofils mindestens eine Rolle zugeteilt. Dieser kann auch einer Gruppe zugeteilt werden. Die Funktions- bzw. Stellenprofile werden durch die jeweils zuständige Organisationseinheit eines Teilnehmers erstellt. Ein Funktions- bzw. Stellenprofil kann mehrere Rollen bzw. Benutzergruppen erhalten. Die jeweils zuständige Organisationseinheit eines Teilnehmers kann Benutzergruppen bilden, in denen mehrere Identitäten und Ressourcen, die aufgrund einer oder mehrerer Gemeinsamkeiten eine Einheit bilden, zusammengefasst werden können. Eine Rolle bzw. Benutzergruppe kann in sich selber wiederum mehrere Berechtigungen haben.

Berechtigungssteuerndes Merkmal bei einer gruppenbasierten Berechtigungssteuerung ist die Zugehörigkeit der Identität zu einer bestimmten Gruppe. Es werden mehrere Identitäten in einer Gruppe zusammengefasst, die über eine Gemeinsamkeit verfügen. Anders als bei der Attributsteuerung müssen keine Daten bei der Identität geführt werden. Benutzergruppen lassen sich grundsätzlich einfacher steuern als Rollen, es sei denn, es wird eine unübersichtliche Anzahl an Gruppen gebildet. Beim Anlegen der Benutzergruppen ist darauf zu achten, dass

* die Bezeichnung der Gruppe innerhalb eines Mandanten eindeutig ist,
* Klarheit über die Quelle der Identitäten besteht,
* Klarheit über den Eigentümer (Verantwortlichen) der Quelle besteht,
* die Daten in einer hinreichend guten Qualität vorliegen und
* der Pflegeprozess der Daten organisiert ist.

Zusätzlich zu Rollen und Benutzergruppen können Attribute zur Berechtigungssteuerung verwendet werden. Die Attribute müssen zu den Berechtigungen passen, indem sie exakt den Kreis der Identitäten adressieren, die die Berechtigung besitzen sollen. So können Attribute beispielsweise für die Zuordnung zu einem Mandanten, für die Standortzuordnung und für die Zuordnung zu bestimmten Verfahren, Ordnern oder Dokumenten verwendet werden. Für die Attributverwaltung ist es wichtig, dass Klarheit darüber besteht, woher die Attribute und ihre Werte kommen, wer sie nach welchen Kriterien pflegt und wie aktuell sie sind. Außerdem muss die Struktur der Attributwerte über die Zeit konsistent gehalten werden, damit es nicht zu aufwendigen Anpassungen kommt. Es sollte daher ausreichend Platz für Daten eingeräumt werden. Für die Attributwerte können auch Kürzel genutzt werden.

Die Beantragung erfolgt bei der jeweils zuständigen Organisationseinheit eines Teilnehmers. Die Freigabe basiert auf einer Informationssicherheits- und Datenschutz-Prüfung (ISDS-Prüfung). Bei der Prüfung stehen die Rechtmäßigkeit, die Verhältnismäßigkeit und die Umsetzung des Need-to-Know-Prinzips im Vordergrund. Es muss zudem ausgeschlossen werden, dass durch die Rollenkumulation unvorhergesehene Berechtigungen erteilt bzw. unvereinbare Rollenprofile zusammengeführt werden.

Die technische Umsetzung der Rollen- und Benutzergruppenzuteilung muss im 4-Augen-Prinzip erfolgen. Das heißt, nach der Erstellung ist ein vollständiger Test separat durch eine zweite Person durchzuführen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Beantragung** | **Genehmigung** | **Umsetzung** |  |
| Identität | **Beantragungsinstanz** | **Freigabe- instanz** | **technische Bereitstellung** |  |
| **Funktionsprofil/Attribute** | **Zuweisungsverfahren Benutzer/Rolle/ Gruppe/Attribute** | **Antragsfreigabeverfahren** | **Erstellungsverfahren** | Rollen-/Benutzergruppenzuteilung |
| **Rollen-/Grup- penkatalog** | **Bedienstetenverzeichnis** | **ISDS-Prüfung** | **Test** |  |
|  | **Antrag** | **Freigabe/Rückweisung** | **Betrieb** |  |

**Abbildung: Rollen-/Benutzergruppenzuteilung**

Auf dieser Grundlage erfolgt eine strukturierte und überprüfbare Berechtigungsvergabe.

## Rollentrennung

Es wird im Folgenden festgelegt, welche Rollen voneinander zu trennen sind:

* Es erfolgt eine Wahrnehmung administrierender und sachbearbeitender Rollen.
* Operationelle (z. B. Administration und Sachbearbeitung) und beaufsichtigende Rollen (z. B. Fach- und Rechtsaufsicht, Datenschutzbeauftragter, Informationssicherheitsbeauftragter) sind zu trennen, um Selbstkontrolle und mithin ein erhöhtes Missbrauchsrisiko zu vermeiden.

Kann eine personelle Trennung nicht gewährleistet werden, so dass eine Person zwei voneinander zu trennende Rollen wahrnimmt, so muss eine organisatorische Trennung durch getrennte Benutzerkonten erfolgen. Zwischen verschiedenen beaufsichtigenden Rollen muss eine personelle Trennung erfolgen.

Die jeweils zuständige Stelle der Teilnehmer kann eine weitergehende Rollentrennung festlegen. Die zuständigen Stellen eines Teilnehmers sind dafür verantwortlich, dass die Vorgaben für die Rollentrennung in der E-Akten-Lösung des Teilnehmers umgesetzt werden. Die technische Umsetzung erfolgt durch den fachlichen Administrator des jeweiligen Teilnehmers.

## Berechtigungsvergabe

Jeder Benutzer erhält die für seine Tätigkeit erforderlichen Berechtigungen von der jeweils zuständigen Stelle eines Teilnehmers. Es dürfen immer nur die Zugriffsrechte vergeben werden, die für die Aufgabenwahrnehmung des einzelnen Benutzers notwendig sind (Principle of Least Privilege). Dabei ist die Einhaltung der Rollentrennung zu beachten. Berechtigungen können für Verfahren, Akten, Teilakten und Dokumente vergeben werden. Auch eine teilnehmerübergreifende Vergabe von Rechten muss gewährleitet werden.Falls die zugeteilten Standardberechtigungen der Rollen für einzelne Benutzer eingeschränkt werden sollen, ist dies von der verantwortlichen Stelle des Teilnehmers zu veranlassen und von lokalen Administrator des Teilnehmers umzusetzen. Sofern temporäre Berechtigungen zum Einsatz kommen, ist sicherzustellen, dass dies nur geschieht, wenn es erforderlich ist und dass diese Berechtigungen von der Stelle, welche die Berechtigung vergeben hat, überwacht werden. Der ordnungsgemäße Entzug (Beendigung, auch bei auf Zeit vergebenen Berechtigungen, die automatisch auslaufen) der Berechtigung ist sicherzustellen und zu dokumentieren.Die Zuweisung der Rollenberechtigungen auf die entsprechenden IT-Ressourcen ist ein operativer Prozess, der klar definierten Abläufen folgen muss. Als Ausgangspunkt dient der Rollenkatalog, der die Berechtigungen der einzelnen Rollen dokumentiert. Die in den Rollen enthaltenen Berechtigungen werden dann technisch auf die Ressourcen angewandt.

Nach der technischen Umsetzung der Berechtigungsvergabe sind die Berechtigungen der Rollen ausführlich zu testen. Dabei sind nicht nur die Einzelrollen, sondern auch die Kombinationen zu kontrollieren, bevor diese dem Betrieb übergeben werden. Es sind Testprozesse in der Pre-Produktionsumgebung mit entsprechender Dokumentation zu etablieren.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Beantragung** | **Genehmigung** | **Umsetzung** |  |
|  | **Beantragungsinstanz** | **Freigabe- instanz** | **technische Bereitstellung** |  |
| **Rollen-/Gruppenkatalog** | **Berechtigungsmatrix** | **Funktionale Prüfung** | **technische Umsetzung** | Rolle/  Benutzergruppe/  Ressource |
|  | **Berechtigungsstufe** | **System-Prüfung** | **Test** |  |
|  |  |  | **Betrieb** |  |

**Abbildung: Berechtigungsvergabe**

Für die Berechtigungsvergabe sollten Berechtigungsstufen verwendet werden. Sie erstrecken sich von „Kein Zugriff“ bis zum „Vollzugriff“ und beziehen sich auf die Aktionsarten. Es können aber auch einzelne Ressourcen (Funktionen und Inhalte) einbezogen werden. Die definierten Berechtigungsstufen ermöglichen die Berechtigungsvergabe durch die Angabe der Ziffer der Berechtigungsstufe, die über ein berechtigungssteuerndes Element (z. B. Rolle oder Gruppe) an die Identität vergeben wird.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | |  | |  | |  | |
| **0** | **Kein Zugriff** | **3** | **Vergleichen** | **6** | **Hinzufügen** | **9** | **Ausführen** | **12** | **Vollzugriff** |
| **1** | **Entdecken** | **4** | **Darstellen/Zeigen** | **7** | **Ändern** | **10** | **Abbrechen** |  |  |
| **2** | **Suchen** | **5** | **Lesen/Öffnen** | **8** | **Löschen** | **11** | **Schreiben** |  |  |

Werden mehrere Elemente (Rollen, Benutzergruppen und Attribute) zur Berechtigungssteuerung verwendet, so müssen sie mittels Verknüpfungselementen im Rahmen des Provisioning miteinander verknüpft werden. Das Verknüpfungselement kann über mehrere Eingänge verfügen, aber nur über einen einzigen Ausgang. Über die Eingänge geben Zustände bestimmte Bedingungen (Conditions) ein, die logisch miteinander verknüpft werden (z. B. UND, ODER, NICHT, UND NICHT, ODER NICHT, EXLUSIV ODER, ÄQUIVALENZ). Durch die Verknüpfung ergibt sich am Ausgang ein berechtigungserteilender oder -verweigernder Zustand. Erfolgt die Berechtigungssteuerung über eine Vielzahl von Merkmalen, so speisen die Elemente die Zustände in das Regelwerk (Rule Engine) ein, das die einzelnen Regeln (Policy Rules) der Zugriffspolitik (Access Policy) enthält. Die im Regelwerk verarbeiteten Regeln bilden die Grundlage für die Berechtigungsentscheidung.

Durch Worksets oder Arbeitsplatzprofile kann eine große Anzahl von Berechtigungen freigeschaltet oder gesperrt werden. Arbeitsplatzprofile zeichnen sich dadurch aus, dass die Entscheidung über Berechtigungen bereits im Planungsprozess getroffen werden und keine Bedingungsprüfung mehr erfolgen muss. Dadurch erlischt aber die Dynamik des Regelwerks.

Die Zergliederung von Funktionen in einzelne Rollen und Funktionalitäten kann bei Bedarf durch Zerlegung der Funktionalitäten in einzelne Prozessschritte verfeinert werden. Aufgrund des hohen Verwaltungsaufwands sollte dies nur in sensiblen Bereichen erfolgen, um das „Need-to-Know“-Prinzip umzusetzen.

## Schützenswerte/ geheimhaltungsbedürftige Verfahren

und im Benutzerkonto hinterlegt sein

## r

## Changemanagement

Auslöser für Änderungen der Berechtigungen können vielfältiger Natur sein. Häufig erfordert ein Wechsel der Funktion, der Organisationseinheit oder auch des Status der Daten eine Anpassung der Berechtigungen. Die Rollen- und Gruppenmitgliedschaften sind zu überprüfen, wenn sich die Aufgabe oder die Organisationseinheit eines Benutzers ändert. Die Änderungen der Rollen und Berechtigungen haben klare Verantwortlichkeiten und unterliegen einem definierten Änderungsprozess bei jedem Verantwortlichen. Grundlegende Änderungen des Rechte- und Rollenkonzepts der E-Akten-Lösung werden durch die Verantwortlichen beschlossen und innerhalb des Programms Polizei 20/20 umgesetzt.

Alle Änderungen sind zu dokumentieren. Die mit den Änderungen betrauten Personen sind bezeichnet und haben nur eine Leseberechtigung auf die entsprechenden Logeinträge (Nachvollziehbarkeit).

## Administration der Berechtigungen

Die Benutzerkonten, Rollen, Benutzergruppen, Berechtigungen usw. werden auf Veranlassung des jeweiligen Verantwortlichen administriert. Bei der Administration sind die datenschutz- und datensicherheitsrelevanten Vorgaben der Verantwortlichen, die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik, die einschlägigen Vorgaben und Empfehlungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sowie die gängigen Normen und Standards zu beachten.

## Dokumentation der Zugriffsrechte

Zur Gewährleistung der Nachvollziehbarkeit und Verantwortlichkeiten bei den Zugriffsrechten, sind die Rollen- und Berechtigungsvergaben von der für die Benutzerverwaltung zuständigen Stelle des Teilnehmers zu dokumentieren.. Die Zuweisung der Zugriffsrechte und die Benutzer mit ihren Rollen und Berechtigungen sind aufzuführen. Die Dokumentation ist laufend und zeitnah zu aktualisieren. Es ist wichtig, dass nur ein Original dieser Dokumentation besteht, von dem alle weiteren Prozesse und Systeme (z. B. das Active Directory) die Daten beziehen können.

Folgende Informationen sollten mindestens dokumentiert werden:

* die für die Definition und Zuweisung der jeweiligen Rolle verantwortlichen Stellen und Personen,
* Zuordnung der Benutzer zu einer Rolle,
* Berechtigung eines Benutzers aus der Rollenzuweisung,
* Art der Benutzerkennung eines Benutzers,
* Semantik der Benutzerkennung eines Benutzers,
* Rollenkonflikte und deren Lösung,
* korrekte Durchführung administrativer Aufgaben,
* Einzelberechtigungen eines Benutzers,
* zeitliche Begrenzung einer Berechtigung,
* administrative Aufgaben für die Verwaltung einer Rolle,
* Verfahren zur Beantragung, Festlegung, Freigabe, technischen Bereitstellung und Veränderung von Zugriffsrechten,
* Kontrollen und ihre Ergebnisse,
* Information der verantwortlichen Stelle bei festgestellten Abweichungen,
* Maßnahmen zur Behebung künftiger Abweichungen,
* Entzug einer Berechtigung.

Die Dokumentation darf nur von dazu befugten Personen bewirtschaftet werden. Andere Personen erhalten nur Lesezugriff, soweit dies erforderlich ist. Die Dokumentation wird im Backupzyklus zwecks Nachvollziehbarkeit der Berechtigungen mit definierter Aufbewahrungsdauer gespeichert.

## Kontrolle der Berechtigungen

Um die Aktualität der Berechtigung zu gewährleisten und Missbrauch zu vermeiden, sind die Berechtigungen regelmäßig durch die jeweils zuständige Stelle eines Teilnehmers zu überprüfen. Die zugewiesenen Berechtigungen sowie die Funktionen und Rollen werden durch den jeweiligen Verantwortlichen zyklisch (abhängig von der Vertraulichkeits-klassifizierung), mindestens jährlich, und bei Anlass kontrolliert.

Bei den Kontrollen sind regulatorische, technische und organisatorische Faktoren zu berücksichtigen, die eine Anpassung der Berechtigungen mit sich bringen können. Neben der Kontrolle des aktuellen Zustandes ist ein besonderes Augenmerk auf neue Schnittstellen und Datenflüsse zu legen, insbesondere solche, die das bestehende Rechte- und Rollenkonzept aushebeln und Personen Zugriffsmöglichkeiten verschaffen können, die nicht erlaubt sind.

Die Kontrollen sind durch die jeweils zuständige Organisationseinheit eines Teilnehmers zu dokumentieren und daraus resultierende Handlungsnotwendigkeiten zu ergreifen.

## Kontrolle der Zugriffe und Protokolldateien

Die Verantwortlichen sind als Informationseigner auch verantwortlich für interne Kontrollen der Zugriffe nach dem Need-to-Know-Prinzip. Bei Zugriffen auf personenbezogene Daten (auch nur lesende) ist eine Protokollierung notwendig. Die Protokollierung hat die Zielsetzung, den ordnungsgemäßen Betrieb zu überwachen, Fehlerzustände möglichst frühzeitig zu erkennen und den ordnungsgemäßen Umgang mit informationstechnischen Einrichtungen zu dokumentieren. Fehlgeschlagene Anmeldeversuche können auf die Nichtbeachtung des Berechtigungskonzeptes oder Manipulationsversuche hindeuten. Protokollaufzeichnungen werden daher regelmäßig geprüft.

Die auf den Zugriffsprotokollen basierenden internen Kontrollen dienen der Kontrolle der Rechtmäßigkeit der Zugriffe anhand der Geschäftsfälle (zweckgebunden). Diese kompensierende Maßnahme ist auch notwendig, wenn z.B. aufgrund von applikatorischen Einschränkungen das Need-to-Know-Prinzip nicht auf die Granularität der Berechtigungen abgebildet werden kann. Hierbei muss beachtet werden, dass die Kontrolle nachvollziehbar ist und mittels eines Stichprobenverfahrens erfolgt. Dazu kommt, dass nicht berechtigte Zugriffe auch dienstrechtliche bzw. strafrechtliche Konsequenzen haben können. Es muss berücksichtigt werden, dass diese Kontrolle nicht zu einer systematischen Überwachung der Mitarbeitenden führen darf. Kompensierende Maßnahmen wie die nachträgliche Kontrolle können eine optimale Zugriffssteuerung ausschließlich ergänzen, nicht aber ersetzen.

Administratoren können einen besonderen Einfluss auf die Strukturen eines IT-Systems ausüben, weshalb sie bei der Nutzung administrativer Rechte einer besonderen Kontrolle unterliegen. Die Nutzung administrativer Rechte muss zu einem Eintrag im Protokoll führen, der von den Administratoren selbst nicht verändert oder umgangen werden kann.

Damit die Kontrollen durchgeführt werden können, werden schon bei der Anforderung an Systeme in der Spezifikation die Anforderungen an die Protokollierung in einem Protokollierungskonzept definiert. Dabei ist der Zweckbindung, der Verhältnismäßigkeit und der Datenminimierung Rechnung zu tragen. Solche Protokolle dürfen nur für den Zweck der Überprüfbarkeit der Einhaltung der Zweckbestimmung einer Datenbearbeitung verwendet werden. Der Zugriff auf Protokollinformationen (Logs) unterliegt auch dem Need-to-Know-Prinzip und daraus folgenden Anforderungen an die Berechtigungssteuerung.

## Benutzung von privilegierten Benutzerkonten

Die Benutzung und Aktualität privilegierter Benutzerkonten, das heißt Konten mit erweiterten Rechten und Berechtigungen, wie etwa Administratoren, sind regelmäßig zu überprüfen.

Jede administrative Kennung kann eindeutig einem Bediensteten bzw. Mitarbeiter eines Verantwortlichen oder Auftragsverarbeiters oder einem technischen Benutzer (Systemkonten und Dienstkonten) zugeordnet werden. Die Nutzung eines Kontos von mehreren Bediensteten bzw. Mitarbeitern ist stets zu vermeiden, da hier keine Nachvollziehbarkeit gegeben ist. Eine entsprechende Dokumentation ist vorhanden.

Eine Regelung zum Umgang mit höher privilegierten Berechtigungen ist in schriftlicher Form zu dokumentieren. Administrative Konten haben aus der Funktionalität heraus Zugriff auf alle Details eines IT-Systems, einer Anwendung oder Datenbank für die diese Berechtigung vergeben wurde. Eine besondere Verpflichtung zur regelmäßigen Kontrolle durch neutrale Instanzen ist daher unverzichtbar.

Technische Benutzer verfügen über die mit Abstand umfangreichsten Berechtigungen. Diese müssen separat von anderen Rollen und administrativen Konten angelegt werden und die Passwörter hierzu stets nur den verantwortlichen Personen bekannt sein. Eine Hinterlegung in einem verschlossenen Umschlag im Tresor oder digital verschlüsselt in einer entsprechenden Passwortsicherungssoftware ist notwendig. Diese Konten dürfen keinesfalls für die Administration verwendet werden oder deren Passworte der Administration bekannt sein.

## Fehlgeschlagene Zugriffsversuche und Berechtigungs-verstöße

Sofern verdächtige bzw. unregelmäßige Zugriffe auf Verzeichnisse, Dateien oder die Registrierung festgestellt wurden, ist das jeweilige Sicherheitsprotokoll der Anwendung zu überprüfen. Werden Auffälligkeiten oder Berechtigungsverstöße festgestellt, muss deren Ursache ermittelt werden. Hierfür wird vorab durch die für die IT-Sicherheit zuständige Stelle festgelegt, ab wann Ereignisse als auffällig anzusehen sind.

## Entzug von Berechtigungen

Arbeitet eine Person nicht länger mit der E-Akten-Lösung (z. B. Entfernung aus dem Dienstverhältnis, Kündigung, Ruhestand, zeitlich begrenzte Tätigkeit), so ist durch die jeweils zuständige Organisationseinheit eines Teilnehmers in einem Verfahren sicher zu stellen, dass alle verbundenen Berechtigungen aus diesem IT-System (und ggf. aus anderen IT-Systemen) gesperrt und entfernt werden. Es ist sicherzustellen, dass inaktive Benutzerkonten nach einem angemessenen Zeitraum gesperrt bzw. vom System gelöscht werden. Gelten bestimmte Berechtigungen nur für einen gewissen Zeitraum, müssen diese Berechtigungen regelmäßig durch die jeweils zuständige Organisationseinheit eines Teilnehmers überprüft werden, um zu gewährleisten, dass sie fristgerecht wieder entzogen werden.

# Funktionen von e²A und Anpassungsbedarf

Die Funktionen zum Verwalten von Rechten und Rollen in e²A sind dem „e²A Integrationsleitfaden“, der „e²A Benutzeranleitung“ und der „e²A Fachadministration“ zu entnehmen.

Das Rechte- und Rollenkonzept muss insbesondere auf die Feinplanung und die Vorgaben des IAM-Dienstes abgestimmt werden. Dies kann dazu führen, dass die Vorgaben für die Authentifizierung und Autorisierung, die Rollenprofile und die Regelungen für die Berechtigungsverwaltung ggf. noch geschärft, angepasst oder ergänzt werden.

Es erfolgt eine Anpassung der Berechtigungsfunktionen von e²A an die Vorgaben des Rechte- und Rollenkonzepts der E-Akten-Lösung. Anpassungsnotwendigkeiten können insbesondere bei der Anbindung des IAM-Dienstes und der Berechtigungssysteme der Teilnehmer, bei der Adaption der Rollen- und Gruppenprofile der Polizeien und des Zolls und bei der technischen Umsetzung der Berechtigungsverwaltung bestehen. Dies wird im Einzelnen mit den Auftragsverarbeitern (Weiterentwicklung und Betrieb der E-Akten-Lösung) abgestimmt und bei der Fortschreibung des Rechte- und Rollenkonzepts berücksichtigt.

# Zentrale Erreichbarkeit

Das Projekt Elektronische Akte in Strafsachen im Programm Polizei 20/20 ist erreichbar unter:

Projektbüro: Bundespolizeipräsidium

Adresse: Heinrich-Mann-Allee 103, 14473 Potsdam

E-Mail: bpolp.e-strafakte@polizei.bund.de

Telefon: 0331-979970

# Anlage 1 – Begriffsdefinitionen

Nachfolgend werden grundlegende Begriffe dieses Konzeptes definiert:

1. Benutzer (User)

Ein Benutzer ist eine Person, die in der Organisation des Verantwortlichen oder des Auftragsverarbeiters auf die E-Akten-Lösung zugreift und diese nutzt. Für jeden Benutzer ist mindestens ein Benutzerkonto mit bestimmten Identitäten vorhanden. Ein Benutzerkonto darf nur einem Benutzer zugeordnet sein.

Jeder Benutzer entspricht einer festgelegten Entität, der eine oder mehrere Rollen, Funktionalitäten, Berechtigungen und Benutzergruppen zugewiesen sind.

1. Entität (Entity)

Entität ist ein eindeutig bestimmtes Informationsobjekt, über das Informationen gespeichert oder verarbeitet werden sollen. Das Objekt kann materiell oder immateriell, konkret oder abstrakt sein (z. B. ein Fahrzeug, eine Person, ein Zustand). Entitäten haben konkrete Ausprägungen (Instanzen) und jeweils eine [Identität](https://de.wikipedia.org/wiki/Identit%C3%A4t).

1. Funktionalität(en)

Funktionalitäten sind die Menge der in einem Rollenprofil vorhandenen Funktionen einer Identität mit festgelegten Eigenschaften.

1. Identität (Identity)

Eine Identität ist eine bestimmte Kombination von Eigenschaften und Rollen eines Benutzers (personelle Identität als physische Instanz, gelebte Identität als Position/en und Funktionalitäten in einer Organisation, kontextuelle Identität als Rolle/n und logische Identität als Zugriffe über Benutzerkonto/en), die mit einem eindeutigen Bezeichner benannt wird. Diese Eigenschaften werden über Attribute festgelegt.

1. Attribute (Attributes)

Attribute sind einzelne Informationen, die einem Objekt (z. B. einer Person) hinzugefügt werden und die dazu verwendet werden, um das jeweilige Objekt zu beschreiben oder zu charakterisieren. Hierzu werden die für einen Zweck wichtigen Informationen ausgewählt und als Attribute dem Objekt zugeordnet. Der Zweck bestimmt sich aus den Anwendungen, die durch die Attribute bedient werden sollen.

1. Rollen (Role)

Durch Rollen wird festgelegt, welche Aufgabe ein Benutzer wahrnimmt und welche Berechtigungen er dazu benötigt. Jede Rolle beschreibt die Funktion des Benutzers, die Daten, auf die dieser zugreifen darf, und die Aktionen, die dieser ausführen darf. Die Rolle bezieht sich auf die Dienststelle des Nutzers. Dieser kann mehrere Rollen wahrnehmen, soweit keine Rollentrennung aus rechtlichen oder organisationsrelevanten Gründen geboten ist. Technische Rollen werden eingesetzt, um Funktionen in der IT-Anwendung zu beschreiben und zu berechtigen.

1. Benutzergruppen (User Groups)

Benutzergruppen können definiert werden, um mehrere Berechtigungen und Identitäten mit einer Gemeinsamkeit zusammenzufassen, so dass alle Mitglieder einer Gruppe über dieselben Befugnisse verfügen. Dadurch werden aufwändige und fehlerhafte Zuweisungen von einzelnen Berechtigungen zu einem Benutzer verhindert.

1. Berechtigung (Authorization)

Eine Berechtigung regelt den Zugriff auf die E-Akten-Lösung und legt fest, welche Aktionen ein Benutzer mit einer Ressource ausführen kann. Für unterschiedliche Objekte können einzelnen Benutzern, Rollen oder Benutzergruppen Berechtigungen zugeordnet werden.

1. Ressourcen (Resources)

Ressourcen sind Objekte, die Funktionen (z. B. Recherche, Analyse oder Konvertierung) und/oder Inhalte (z. B. Dateisystem, Verzeichnisse, Verfahren, Ordner, Akten, Aktenteile, Dokumente und Daten) bereitstellen, die genutzt werden können.

1. Aktionsarten (Types of Action)

Für Ressourcen (Funktionen und/oder Inhalte) können folgende Aktionsarten freigegeben oder gesperrt werden:

1. Lesen/Öffnen (Read/Open)

Die Berechtigung zum Lesen/Finden erlaubt es dem Benutzer, auf den Inhalt der Ressource zuzugreifen. Dokumente/Dateien dürfen geöffnet und der Inhalt angezeigt und/oder ausgelesen werden. Attribute und Verwaltungsinformationen der Ressource können angezeigt werden.

Die Leseberechtigung schließt die Berechtigung zum Darstellen/Zeigen (Show), Vergleichen (Compare), Suchen (Search/Find) und Entdecken (Detect) mit ein. Darstellen/Zeigen ermöglicht es dem Benutzer, sich die Inhaltsressource anzeigen zu lassen (z. B. in einem Verzeichnis oder einer Liste) ohne dass sie geöffnet und gelesen werden kann. Vergleichen gestattet es dem Benutzer, Vergleiche zwischen Inhaltsressourcen durchzuführen, ohne diese darzustellen oder zu lesen. Die Vergleichsberechtigung schließt die Berechtigung zum Entdecken mit ein. Suchen erlaubt es dem Benutzer, nach Inhaltsressourcen, deren Ablageort unbekannt ist, zu suchen. Die Suchberechtigung schließt die Berechtigung zum Entdecken mit ein. Entdecken ermöglicht es dem Benutzer, die Existenz der jeweiligen Funktions- und/oder Inhaltsressource festzustellen, auf die sich die Berechtigung zum Entdecken bezieht.

1. Schreiben (Write)

Die Berechtigung zum Schreiben umfasst die Berechtigungen Lesen/Öffnen, Hinzufügen und Ändern.

Hinzufügen gestattet es dem Benutzer, der Inhaltsressource etwas hinzuzufügen. In der E-Akten-Lösung können beispielsweise Dokumente angelegt und in Dokumente schreibend Inhalte hinzugefügt werden. Die Hinzufügberechtigung schließt die Berechtigungen zum Entdecken und Darstellen mit ein und ist in der Regel mit der Leseberechtigung verbunden.

Ändern ermöglicht es dem Benutzer, Funktionen oder Inhalte der Ressourcen zu verändern. Neue Funktionen oder Inhalte können hinzugefügt oder bestehende Inhalte weggenommen werden. Die Änderungsberechtigung schließt die Berechtigungen zum Hinzufügen und zum Lesen mit ein.

1. Löschen (Delete)

Die Berechtigung zum Löschen erlaubt es dem Benutzer, ein Objekt als Ganzes vollständig zu entfernen. Die Löschberechtigung schließt mindestens die Berechtigung zum Entdecken mit ein.

1. Ausführen (Execute)

Die Berechtigung zum Ausführen gestattet es dem Benutzer, Funktionen oder ausführbare Inhalte einer Ressource zu starten und/oder auszuführen. Einzelne Ausführungsvarianten können mit besonderen Berechtigungen versehen sein. Die Ausführungsberechtigung schließt die Berechtigungen zum Entdecken und Darstellen mit ein.

1. Abbrechen (Abort)

Die Berechtigung zum Abbrechen ermöglicht es dem Nutzer bzw. Administrator, gestartete Funktionen abzubrechen und zum Ausgangszustand zurückzukehren.

1. Organisatorische Anforderungen (Organizational Requirements)

Grundlegende organisatorische Abläufe in Form von definierten Prozessen werden eingerichtet, um eine zuverlässige Verwaltung der Berechtigungen zu gewährleisten.

1. Zugriffsrechte (Access Rights)

Zugriffsrechte beschreiben organisatorische Anforderungen an die Verwaltung (Administration) von Nutzern, Benutzergruppen, Rollen oder Berechtigungen sowie eine nachhaltige Dokumentation.

# Anlage 2 – Entitäten, Aktionsarten und Funktionalitäten des lokalen Administrators

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle   |  | | --- | |  | | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |  |  |
| 1 | Lokaler Administrator | **Administrationsprotokollierung (Logging)** | Ja | Nein | Nein | x | Nein |
| 2 | Lokaler Administrator | **Fachdatenprotokollierung (Datenschutz)** | Ja | Nein | Nein | x | Nein |
| 3 | Lokaler Administrator | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Lokaler Administrator | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Lokaler Administrator | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Lokaler Administrator | **Mandant (eigener)** | Ja | Nein | Nein | x | x |
| 7 | Lokaler Administrator | **Dienststelle** | Ja | Ja | Ja | x | x |
| 8 | Lokaler Administrator | **Benutzergruppen** | Ja | Ja | Ja | x | x |
| 9 | Lokaler Administrator | **Benutzerkonto** | Ja | Ja | Ja | x | x |
| 10 | Lokaler Administrator | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Lokaler Administrator | **Berechtigungen** | Ja | Nein | Nein | Nein | Nein |
| 12 | Lokaler Administrator | **Anwendungsschicht** | Ja | Ja | Ja | Ja | Ja |
| 13 | Lokaler Administrator | **Datenhaltungsschicht** | Nein | Nein | Nein | Nein | Nein |
| 14 | Lokaler Administrator | **Drucken** | Ja | Ja | x | Ja | Ja |
| 15 | Lokaler Administrator | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 16 | Lokaler Administrator | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 17 | Lokaler Administrator | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |

Die nachfolgenden Funktionalitäten werden dem lokalen Administrator gewährt:

* Dienststellen- und Organisationsinformationen erstellen, ändern und löschen,
* zentrale Dokumentenvorlagen einstellen, ändern, löschen,
* Favoritenpool pflegen,
* Funktionsrechte bearbeiten,
* Historie Nutzerzuordnung sehen,
* Integrierte Anwendungen, Funktionalitäten und Tools konfigurieren und verwalten,
* Kataloge pflegen,
* Katalog-Updateverfahren,
* eigenen Mandanten einsehen,
* Metadatenvorlagen (Dienststelle, Abteilung) erstellen, ändern und löschen,
* Benutzereinstellungen bearbeiten,
* Rollen den Benutzerkonten technisch zuweisen,
* Benutzerkonto sperren/entsperren,
* Passwort ändern,
* Passwort Blacklistpflege,
* Postfächer für Verantwortlichen innerhalb der Teilnehmer erstellen, ändern und löschen,
* Protokollierung anzeigen,
* Protokollierung Fachdaten anzeigen,
* Schriftstücktypen (Beschluss, Vermerk, Protokoll, Gutachten) erstellen, ändern und löschen,
* Sessions beenden,
* Symbole (klassisches Design) oder Icon-Farbe (modernes Design) den Schriftstücktypen zuordnen,
* Templates für Ordnerstrukturen erstellen, ändern und löschen,
* Trefferliste editieren,
* Trefferlistenfilter (gespeicherte) verwenden,
* Verfahrensstatistik.

# Anlage 3 – Entitäten, Aktionsarten und Funktionalitäten der Führungskraft

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Führungskraft | **Administrationsprotokollierung (Logging)** | Nein | Nein | Nein | x | Nein |
| 2 | Führungskraft | **Fachdatenprotokollierung (Datenschutz)** | Ja | Nein | Nein | x | Nein |
| 3 | Führungskraft | **Statistik** | Ja | Nein | Nein | x | x |
| 4 | Führungskraft | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Führungskraft | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Führungskraft | **Mandant** | Ja | Nein | Nein | x | x |
| 7 | Führungskraft | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Führungskraft | **Benutzergruppen der Organisationseinheit** | Ja | Nein | Nein | x | x |
| 9 | Führungskraft | **Benutzer der Organisationseinheit** | Ja | Nein | Nein | x | x |
| 10 | Führungskraft | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Führungskraft | **Berechtigungen** | Ja | Ja | Ja | Ja | Ja |
| 12 | Führungskraft | **Posteingang Organisationseinheit** | Ja | Ja | x | Ja | Ja |
| 13 | Führungskraft | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Führungskraft | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | Führungskraft | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | Führungskraft | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Führungskraft | **Verfahrenshistorie** | Ja | Nein | Nein | x | x |
| 18 | Führungskraft | **Ordner** | Ja | Nein | Nein | x | x |
| 19 | Führungskraft | **Unterordner im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 20 | Führungskraft | **Dokumente im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 21 | Führungskraft | **Kennzeichnung im Ordner „Akte“** | Ja | Nein | Nein | Nein | Nein |
| 22 | Führungskraft | **Metadaten**  im Ordner „Akte“ | Ja | Nein | Nein | x | x |
| 23 | Führungskraft | **Unterordner in anderen Ordnern** | Ja | Nein | Nein | x | x |
| 24 | Führungskraft | **Dokumente in anderen Ordnern** | Ja | Nein | Nein | x | x |
| 25 | Führungskraft | **Metadaten zu Unterordnern/Dokumenten in anderen Ordnern** | Ja | Nein | Nein | x | x |
| 26 | Führungskraft | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | Führungskraft | **Annotationen** | Ja | Nein | Nein | Nein | Nein |
| 28 | Führungskraft | **Paginieren** | Ja | Nein | x | Nein | x |
| 29 | Führungskraft | **Papierkorb** | Ja | Nein | Nein | x | x |
| 30 | Führungskraft | **Repräsentat** | Ja | Nein | Nein | x | x |
| 31 | Führungskraft | **Verfahrensabgabe** | Ja | Nein | Nein | Ja | Ja |
| 32 | Führungskraft | **Workflow** | Ja | Ja | Ja | Ja | Ja |
| 33 | Führungskraft | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Führungskraft | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Führungskraft | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Führungskraft | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Führungskraft | **weitere Funktionalitäten** | x | x | x | x | x |

Die nachfolgenden Funktionalitäten werden der Führungskraft gewährt:

* Mitzeichnung, Freigabe, Schlusszeichnung,
* Posteingang (Organisationseinheit) verwalten (Einsichtnahme, Weiterleitung und Zurückweisung ggf. mit Begründung, Kennzeichnung als „gelesen“, „ungelesen“, „wichtig“, „Eilsache“),
* Verfahren abgeben,
* Verfahren an Organisationseinheit, verantwortlichen Sachbearbeiter, beteiligten Sachbearbeiter, Sachbearbeiterteam zuweisen,
* Verfahrensstatistik,
* Zeichnungsvorbehalt anbringen,
* Zugriff (lesend) auf Metadaten in Verfahren,
* Zugriff (lesend) auf Verfahrenshistorie und Versionierung,
* ggf. Zugriff (lesend) auf Protokolldaten von Verfahren grundsätzlich nach dem 4-Augen-Prinzip,
* Zugriff (lesend) auf Verfahren,
* Ansicht konfigurieren und speichern,
* Aufgaben (persönlich) erstellen, darstellen und bearbeiten,
* Workflow erstellen, speichern, starten, ändern und abbrechen,
* Dokumente zur weiteren Bearbeitung sperren bzw. signieren,
* Rolle innerhalb der Verfahren hinzufügen, ändern und löschen (verantwortlicher Sachbearbeiter, beteiligter Sachbearbeiter),
* Rechte (Lese- und Schreibrechte bzw. ausschließlich Leserechte) und Gastzugänge an andere Organisationseinheit außerhalb des eigenen Teilnehmers vergeben,
* Suche und Filtern innerhalb der Verfahren und der Metadaten der unterstellten Sachbearbeiter;
* Kontrolle der Nutzung der Funktion für den maschinellen Abgleich personenbezogener Daten mit elektronischen Akten oder elektronischen Aktenkopien durch den verantwortlichen Sachbearbeiter (4-Augen-Prinzip),
* Kontrolle des Löschens ganzer Verfahren und Ordner (4-Augen-Prinzip)
* Kontrolle der Übermittlung von Dokumenten/Dateien aus einem Verfahren (Strafverfahren, Bußgeldverfahren) bei Zweckänderung (4-Augen-Prinzip),
* Setzen eines Verfahrens, Ordners, Dokuments auf „Verborgen“,
* Recht einen Stellvertreter zu bestimmen.

# Anlage 4 – Entitäten, Aktionsarten und Funktionalitäten der Führungskraft mit eingeschränkten Befugnissen

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Führungskraft mit eingeschränkten Befugnissen | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Führungskraft mit eingeschränkten Befugnissen | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Führungskraft mit eingeschränkten Befugnissen | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Führungskraft mit eingeschränkten Befugnissen | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Führungskraft mit eingeschränkten Befugnissen | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Führungskraft mit eingeschränkten Befugnissen | **Mandant** | Ja | Nein | Nein | x | x |
| 7 | Führungskraft mit eingeschränkten Befugnissen | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Führungskraft mit eingeschränkten Befugnissen | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Führungskraft mit eingeschränkten Befugnissen | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Führungskraft mit eingeschränkten Befugnissen | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Führungskraft mit eingeschränkten Befugnissen | **Berechtigungen** | Ja | Ja | Ja | Ja | Ja |
| 12 | Führungskraft mit eingeschränkten Befugnissen | **Posteingang OE** | Ja | Ja | x | Ja | Ja |
| 13 | Führungskraft mit eingeschränkten Befugnissen | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Führungskraft mit eingeschränkten Befugnissen | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | Führungskraft mit eingeschränkten Befugnissen | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | Führungskraft mit eingeschränkten Befugnissen | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Führungskraft mit eingeschränkten Befugnissen | **Verfahrenshistorie** | Ja | Nein | Nein | x | x |
| 18 | Führungskraft mit eingeschränkten Befugnissen | **Ordner** | Ja | Nein | Nein | x | x |
| 19 | Führungskraft mit eingeschränkten Befugnissen | **Unterordner im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 20 | Führungskraft mit eingeschränkten Befugnissen | **Dokumente im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 21 | Führungskraft mit eingeschränkten Befugnissen | **Kennzeichnung im Ordner „Akte“** | Ja | Nein | Nein | Nein | Nein |
| 22 | Führungskraft mit eingeschränkten Befugnissen | **Metadaten**  im Ordner „Akte“ | Ja | Nein | Nein | x | x |
| 23 | Führungskraft mit eingeschränkten Befugnissen | **Unterordner** in anderen Ordnern | Ja | Nein | Nein | x | x |
| 24 | Führungskraft mit eingeschränkten Befugnissen | **Dokumente**  in anderen Ordnern | Ja | Nein | Nein | x | x |
| 25 | Führungskraft mit eingeschränkten Befugnissen | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Nein | Nein | x | x |
| 26 | Führungskraft mit eingeschränkten Befugnissen | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | Führungskraft mit eingeschränkten Befugnissen | **Annotationen** | Ja | Nein | Nein | Nein | Nein |
| 28 | Führungskraft mit eingeschränkten Befugnissen | **Paginieren** | Ja | Nein | x | Nein | x |
| 29 | Führungskraft mit eingeschränkten Befugnissen | **Papierkorb** | Ja | Nein | Nein | x | x |
| 30 | Führungskraft mit eingeschränkten Befugnissen | **Repräsentat** | Ja | Nein | Nein | x | x |
| 31 | Führungskraft mit eingeschränkten Befugnissen | **Verfahrensabgabe** | Ja | Nein | Nein | Ja | Ja |
| 32 | Führungskraft mit eingeschränkten Befugnissen | **Workflow** | Ja | Ja | Ja | Ja | Ja |
| 33 | Führungskraft mit eingeschränkten Befugnissen | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Führungskraft mit eingeschränkten Befugnissen | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Führungskraft mit eingeschränkten Befugnissen | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Führungskraft mit eingeschränkten Befugnissen | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Führungskraft mit eingeschränkten Befugnissen | **weitere Funktionalitäten** | x | x | x | x | x |

# Anlage 5 – Entitäten, Aktionsarten und Funktionalitäten des verantwortlichen Sachbearbeiters

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Verantwortlicher Sachbearbeiter | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Verantwortlicher Sachbearbeiter | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Verantwortlicher Sachbearbeiter | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Verantwortlicher Sachbearbeiter | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Verantwortlicher Sachbearbeiter | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Verantwortlicher Sachbearbeiter | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Verantwortlicher Sachbearbeiter | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Verantwortlicher Sachbearbeiter | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Verantwortlicher Sachbearbeiter | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Verantwortlicher Sachbearbeiter | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Verantwortlicher Sachbearbeiter | **Berechtigungen** | Ja | Ja | Ja | Ja | Ja |
| 12 | Verantwortlicher Sachbearbeiter | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | Verantwortlicher Sachbearbeiter | **Verfahren** | Ja | Ja | Ja² | x | x |
| 14 | Verantwortlicher Sachbearbeiter | **Bearbeitungsstatus** | Ja | Ja | x | x | x |
| 15 | Verantwortlicher Sachbearbeiter | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | Verantwortlicher Sachbearbeiter | **Metadaten zum Verfahren** | Ja | Ja | Ja | x | x |
| 17 | Verantwortlicher Sachbearbeiter | **Verfahrenshistorie** | Ja | Nein | Nein | x | x |
| 18 | Verantwortlicher Sachbearbeiter | **Ordner** | Ja | Ja | Ja | x | x |
| 19 | Verantwortlicher Sachbearbeiter | **Unterordner im Ordner „Akte“** | Ja | Ja\*\* | Ja\*\* | x | x |
| 20 | Verantwortlicher Sachbearbeiter | **Dokumente im Ordner „Akte“** | Ja | Ja\*\* | Ja\*\* | x | x |
| 21 | Verantwortlicher Sachbearbeiter | **Kennzeichnung im Ordner „Akte“** | Ja | Ja | Ja | x | x |
| 22 | Verantwortlicher Sachbearbeiter | **Metadaten**  im Ordner „Akte“ | Ja | Ja\*\* | Ja\*\* | x | x |
| 23 | Verantwortlicher Sachbearbeiter | **Unterordner** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 24 | Verantwortlicher Sachbearbeiter | **Dokumente** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 25 | Verantwortlicher Sachbearbeiter | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Ja | Ja | x | x |
| 26 | Verantwortlicher Sachbearbeiter | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | Verantwortlicher Sachbearbeiter | **Annotationen** | Ja | Ja | Ja | Ja | Ja |
| 28 | Verantwortlicher Sachbearbeiter | **Paginieren** | Ja | Nein | x | Nein | x |
| 29 | Verantwortlicher Sachbearbeiter | **Papierkorb** | Ja | Ja | Ja | x | x |
| 30 | Verantwortlicher Sachbearbeiter | **Repräsentat** | Ja | Nein | Ja | x | x |
| 31 | Verantwortlicher Sachbearbeiter | **Verfahrensabgabe** | Ja | Ja | Ja | Ja\* | Ja\* |
| 32 | Verantwortlicher Sachbearbeiter | **Workflow** | Ja | Ja | Ja | Ja | Ja |
| 33 | Verantwortlicher Sachbearbeiter | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Verantwortlicher Sachbearbeiter | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Verantwortlicher Sachbearbeiter | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Verantwortlicher Sachbearbeiter | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Verantwortlicher Sachbearbeiter | **weitere Funktionalitäten** | x | x | x | x | x |

Die nachfolgenden Funktionalitäten werden dem verantwortlichen Sacharbeiter gewährt:

* Funktionalitäten der Rahmenanwendung der E-Akten-Lösung ausführen,
* Aufgabensteuerung der E-Akten-Lösung ausführen,
* Aktenanwendungen der E-Akten-Lösung ausführen einschließlich Verfahrenssteuerung, Verfahrens- und Dokumentendarstellung und Nutzung der Werkzeugleistenfunktionen,
* Zugriff (lesend) auf Verfahrenshistorie und Versionierung,
* Ansicht konfigurieren und speichern,
* Aufgaben (persönlich) erstellen, darstellen und bearbeiten,
* Workflow erstellen, speichern, starten, ändern und abbrechen,
* Darstellung von Aktendeckeln, Verfahren und Ordner,
* Nutzung der Funktionen im Kontextmenü des Verfahrens,
* Nutzung der Bearbeitungsfunktionen für Ordner,
* Bearbeitungsstatus des Verfahrens ändern,
* Beibehaltung einer Kopie des Verfahrens nach aktiver Entscheidung,
* Nutzung der Bearbeitungsfunktionen für Dokumente,
* Digitale Ausgangsdokumente Dritter kennzeichnen und löschen,
* Dokumente bearbeiten, zur weiteren Bearbeitung sperren bzw. signieren,
* Dokumente/Dateien aus dem Verfahren exportieren bzw. übermitteln (bei Zweckänderung im 4-Augen-Prinzip über den Vorgesetzten),
* Dokumente/Dateien in Verfahren hinzufügen/Importieren, ändern und löschen,
* Dokumente markieren (gelesen/ungelesen, wichtig, eilt, Original/Kopie),
* Dokumentenversionen (inkl. Versionshistorie) anzeigen und auswählen,
* persönliche Dokumentenvorlagen erstellen, speichern, ändern, nutzen und löschen,
* Empfangsbekenntnis (elektronisch) erstellen und auswählen,
* Favoriten (persönlich) erstellen, speichern und löschen,
* Fristen an beteiligten Sachbearbeiter vergeben,
* Leitdokument erstellen, hinzufügen und auswählen,
* Metadaten zu Verfahren, Ordnern, Dokument/Datei hinzufügen, ändern und löschen,
* Historie und Versionierung des Verfahrens anzeigen,
* Rechte (Lese- und Schreibrechte bzw. ausschließlich Leserechte) an andere Organisationseinheit vergeben,
* andere Bedienstete als beteiligte Sachbearbeiter am gesamten Verfahren oder an bestimmten Ordnern berechtigen, deren Berechtigung ändern oder entziehen,
* Templates für Ordnerstruktur erstellen, speichern, ändern und löschen,
* Nutzung der Suchfunktionen,
* Suche und Filtern innerhalb der eigenen Verfahren (Rolle als verantwortlicher oder beteiligter Sachbearbeiter ist hinterlegt),
* Suche und Filtern von Metadaten innerhalb der eigenen Verfahren (Rolle als verantwortlicher oder beteiligter Sachbearbeiter ist hinterlegt),
* Nutzung der Funktion für den maschinellen Abgleich personenbezogener Daten mit einzelnen, zuvor individualisierten elektronischen Akten oder elektronischen Aktenkopien (im 4-Augen-Prinzip über den Vorgesetzten)
* Tools zur Dokumentenbearbeitung verwenden (Annotationen, Kennzeichnung, Texterschließung, Schwärzung, Kennzeichnung etc.),
* Verfahren abgeben,
* Verfahren inkl. Teilakte und Dokument/Datei bearbeiten (Verschieben, Drucken, Kopieren/duplizieren, verlinken, aufteilen und zusammenführen, umbenennen, strukturieren),
* Verfahren inkl. Teilakten und Dokumente/Dateien hinzufügen, ändern/bearbeiten (auch kopieren, verschieben in andere Verfahren) und löschen (Löschen ganzer Verfahren und Ordner nur im 4-Augen-Prinzip über den Vorgesetzten),
* Verfahren inkl. Ordnern und Dokument/Datei als „Eilvorgang“ kennzeichnen,
* Verfahren inkl. Ordnern und Dokument/Datei zum/r Export, Versand, Abgabe, Weitergabe, Vorlage zur Zuweisung von Schreib- und/oder Leserechten auswählen,
* Verfahren inkl. Ordnern und Dokument/Datei dem Vorgesetzten vorlegen oder weitergeben,
* Zeitpunkt zur automatisierten Abgabe von Dokument/Datei definieren,
* Erstellen und Exportieren von Aktenkopien.

# Anlage 6 – Entitäten, Aktionsarten und Funktionalitäten des Sachbearbeiters Straf- und Bußgeldakte

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Sachbearbeiters Straf- und Bußgeldakte | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Sachbearbeiters Straf- und Bußgeldakte | **Fachdatenprotokollierung** | Ja | Nein | Nein | x | Nein |
| 3 | Sachbearbeiters Straf- und Bußgeldakte | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Sachbearbeiters Straf- und Bußgeldakte | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Sachbearbeiters Straf- und Bußgeldakte | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Sachbearbeiters Straf- und Bußgeldakte | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Sachbearbeiters Straf- und Bußgeldakte | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Sachbearbeiters Straf- und Bußgeldakte | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Sachbearbeiters Straf- und Bußgeldakte | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Sachbearbeiters Straf- und Bußgeldakte | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Sachbearbeiters Straf- und Bußgeldakte | **Berechtigungen** | Ja | Ja | Ja | Ja | Ja |
| 12 | Sachbearbeiters Straf- und Bußgeldakte | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | Sachbearbeiters Straf- und Bußgeldakte | **Verfahren** | Ja | Ja | Nein | x | x |
| 14 | Sachbearbeiters Straf- und Bußgeldakte | **Bearbeitungsstatus** | Ja | Ja | x | x | x |
| 15 | Sachbearbeiters Straf- und Bußgeldakte | **Aktenführungsrecht** | Ja | Ja | Ja | Ja | x |
| 16 | Sachbearbeiters Straf- und Bußgeldakte | **Metadaten zum Verfahren** | Ja | Ja | Nein | x | x |
| 17 | Sachbearbeiters Straf- und Bußgeldakte | **Verfahrenshistorie** | Ja | Nein | Nein | x | x |
| 18 | Sachbearbeiters Straf- und Bußgeldakte | **Ordner** | Ja | Ja | Ja | x | x |
| 19 | Sachbearbeiters Straf- und Bußgeldakte | **Unterordner im Ordner „Akte“** | Ja | Ja\*\* | Ja\*\* | x | x |
| 20 | Sachbearbeiters Straf- und Bußgeldakte | **Dokumente im Ordner „Akte“** | Ja | Ja\*\* | Ja\*\* | x | x |
| 21 | Sachbearbeiters Straf- und Bußgeldakte | **Kennzeichnung im Ordner „Akte“** | Ja | Ja | Ja | x | x |
| 22 | Sachbearbeiters Straf- und Bußgeldakte | **Metadaten**  im Ordner „Akte“ | Ja | Ja\*\* | Ja\*\* | x | x |
| 23 | Sachbearbeiters Straf- und Bußgeldakte | **Unterordner** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 24 | Sachbearbeiters Straf- und Bußgeldakte | **Dokumente** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 25 | Sachbearbeiters Straf- und Bußgeldakte | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Ja | Ja | x | x |
| 26 | Sachbearbeiters Straf- und Bußgeldakte | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | Sachbearbeiters Straf- und Bußgeldakte | **Annotationen** | Ja | Ja | Ja | Ja | Ja |
| 28 | Sachbearbeiters Straf- und Bußgeldakte | **Paginieren** | x | x | x | Ja | Ja |
| 29 | Sachbearbeiters Straf- und Bußgeldakte | **Papierkorb** | Ja | Ja | x | Ja | x |
| 30 | Sachbearbeiters Straf- und Bußgeldakte | **Repräsentat** | Ja | Ja | Ja | x | x |
| 31 | Sachbearbeiters Straf- und Bußgeldakte | **Verfahrensabgabe** | Ja | Ja | Ja | x | x |
| 32 | Sachbearbeiters Straf- und Bußgeldakte | **Workflow** | Ja | Ja | Ja | Ja\* | Ja\* |
| 33 | Sachbearbeiters Straf- und Bußgeldakte | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Sachbearbeiters Straf- und Bußgeldakte | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Sachbearbeiters Straf- und Bußgeldakte | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Sachbearbeiters Straf- und Bußgeldakte | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Sachbearbeiters Straf- und Bußgeldakte | **weitere Funktionalitäten** | x | x | x | x | x |

Gewährte zusätzliche Funktionsrechte:

* Übergeben des Aktenführungsrechts,
* Übernehmen des Aktenführungsrechts.
* Erstellen und Exportieren von Repräsentaten.

# Anlage 7 – Entitäten, Aktionsarten und Funktionalitäten des beteiligten Sachbearbeiters

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | beteiligter Sachbearbeiter | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | beteiligter Sachbearbeiter | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | beteiligter Sachbearbeiter | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | beteiligter Sachbearbeiter | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | beteiligter Sachbearbeiter | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | beteiligter Sachbearbeiter | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | beteiligter Sachbearbeiter | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | beteiligter Sachbearbeiter | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | beteiligter Sachbearbeiter | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | beteiligter Sachbearbeiter | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | beteiligter Sachbearbeiter | **Berechtigungen** | Ja | Nein | Nein | Nein | Nein |
| 12 | beteiligter Sachbearbeiter | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | beteiligter Sachbearbeiter | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | beteiligter Sachbearbeiter | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | beteiligter Sachbearbeiter | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | beteiligter Sachbearbeiter | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | beteiligter Sachbearbeiter | **Verfahrenshistorie** | Ja | Nein | Nein | x | x |
| 18 | beteiligter Sachbearbeiter | **Ordner** | Ja | Nein | Nein | x | x |
| 19 | beteiligter Sachbearbeiter | **Unterordner im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 20 | beteiligter Sachbearbeiter | **Dokumente im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 21 | beteiligter Sachbearbeiter | **Kennzeichnung im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 22 | beteiligter Sachbearbeiter | **Metadaten**  im Ordner „Akte“ | Ja | Nein | Nein | x | x |
| 23 | beteiligter Sachbearbeiter | **Unterordner** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 24 | beteiligter Sachbearbeiter | **Dokumente** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 25 | beteiligter Sachbearbeiter | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Ja | Ja | x | x |
| 26 | beteiligter Sachbearbeiter | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | beteiligter Sachbearbeiter | **Annotationen** | Ja | Ja | Ja | Ja | Ja |
| 28 | beteiligter Sachbearbeiter | **Paginieren** | x | x | x | Ja | Ja |
| 29 | beteiligter Sachbearbeiter | **Papierkorb** | Ja | Nein | x | Nein | x |
| 30 | beteiligter Sachbearbeiter | **Repräsentat** | Ja | Ja | Nein | x | x |
| 31 | beteiligter Sachbearbeiter | **Verfahrensabgabe** | Ja | Nein | Ja | x | x |
| 32 | beteiligter Sachbearbeiter | **Workflow** | Ja | Nein | Nein | Nein | Nein |
| 33 | beteiligter Sachbearbeiter | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | beteiligter Sachbearbeiter | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | beteiligter Sachbearbeiter | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | beteiligter Sachbearbeiter | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | beteiligter Sachbearbeiter | **weitere Funktionalitäten** | x | x | x | x | x |

Gewährte Funktionsrechte:

* Funktionalitäten der Rahmenanwendung der E-Akten-Lösung ausführen,
* Aktionen abbrechen,
* Digitale Ausgangsdokumente Dritter kennzeichnen,
* Dokument/Datei als „Eilvorgang“ kennzeichnen,
* Dokument/Dateien hinzufügen, erstellen, signieren, eigene erstellte ändern und löschen,
* Dokumentenversionen anzeigen und auswählen (inkl. Versionshistorie),
* Metadaten (nur eigen erstellte) erstellen, ändern, löschen,
* Suche und Filtern innerhalb der eigenen Verfahren,
* Suche und Filtern von Metadaten innerhalb der eigenen Verfahren,
* Verfahren inkl. Ordnern und Dokument/Datei versenden (z.B. E-Mail),
* Tools zur Dokumentenbearbeitung für eigene erstellte Dokumente nutzen,
* Ansicht konfigurieren und speichern,
* Aufgaben (persönlich) erstellen, darstellen und bearbeiten,
* Workflow erstellen, speichern, starten, ändern und abbrechen,
* Nutzung der Funktionen im Kontextmenü des Verfahrens,
* Nutzung der Bearbeitungsfunktionen für Dokumente,
* persönliche Dokumentenvorlagen erstellen, speichern, ändern, nutzen und löschen, Favoriten (persönlich) erstellen, speichern und löschen.

# Anlage 8 – Entitäten, Aktionsarten und Funktionalitäten des Bediensteten Elektronische Poststelle/Verwaltung

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Bediensteter Elektronische Poststelle/Verwaltung | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Bediensteter Elektronische Poststelle/Verwaltung | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Bediensteter Elektronische Poststelle/Verwaltung | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Bediensteter Elektronische Poststelle/Verwaltung | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Bediensteter Elektronische Poststelle/Verwaltung | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Bediensteter Elektronische Poststelle/Verwaltung | **Mandant** | Ja | Nein | Nein | x | x |
| 7 | Bediensteter Elektronische Poststelle/Verwaltung | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Bediensteter Elektronische Poststelle/Verwaltung | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Bediensteter Elektronische Poststelle/Verwaltung | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Bediensteter Elektronische Poststelle/Verwaltung | **Rollen** | Nein | Nein | Nein | x | x |
| 11 | Bediensteter Elektronische Poststelle/Verwaltung | **Berechtigungen** | Nein | Nein | Nein | Nein | Nein |
| 12 | Bediensteter Elektronische Poststelle/Verwaltung | **Posteingang OE** | Ja | Ja | x | Ja | Ja |
| 13 | Bediensteter Elektronische Poststelle/Verwaltung | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Bediensteter Elektronische Poststelle/Verwaltung | **Bearbeitungsstatus** | Nein | Nein | x | x | x |
| 15 | Bediensteter Elektronische Poststelle/Verwaltung | **Aktenführungsrecht** | Nein | Nein | Nein | Nein | x |
| 16 | Bediensteter Elektronische Poststelle/Verwaltung | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Bediensteter Elektronische Poststelle/Verwaltung | **Verfahrenshistorie** | Nein | Nein | Nein | x | x |
| 18 | Bediensteter Elektronische Poststelle/Verwaltung | **Ordner** | Nein | Nein | Nein | x | x |
| 19 | Bediensteter Elektronische Poststelle/Verwaltung | **Unterordner im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 20 | Bediensteter Elektronische Poststelle/Verwaltung | **Dokumente im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 21 | Bediensteter Elektronische Poststelle/Verwaltung | **Kennzeichnung im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 22 | Bediensteter Elektronische Poststelle/Verwaltung | **Metadaten**  im Ordner „Akte“ | Nein | Nein | Nein | x | x |
| 23 | Bediensteter Elektronische Poststelle/Verwaltung | **Unterordner** in anderen Ordnern | Nein | Nein | Nein | x | x |
| 24 | Bediensteter Elektronische Poststelle/Verwaltung | **Dokumente** in anderen Ordnern | Nein | Nein | Nein | x | x |
| 25 | Bediensteter Elektronische Poststelle/Verwaltung | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Nein | Nein | Nein | x | x |
| 26 | Bediensteter Elektronische Poststelle/Verwaltung | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | Bediensteter Elektronische Poststelle/Verwaltung | **Annotationen** | Nein | Nein | Nein | Nein | Nein |
| 28 | Bediensteter Elektronische Poststelle/Verwaltung | **Paginieren** | Nein | Nein | x | Nein | x |
| 29 | Bediensteter Elektronische Poststelle/Verwaltung | **Papierkorb** | Nein | Nein | Nein | x | x |
| 30 | Bediensteter Elektronische Poststelle/Verwaltung | **Repräsentat** | Nein | Nein | Nein | x | x |
| 31 | Bediensteter Elektronische Poststelle/Verwaltung | **Verfahrensabgabe** | Nein | Nein | Nein | Nein | Nein |
| 32 | Bediensteter Elektronische Poststelle/Verwaltung | **Workflow** | Ja | Ja | Ja | Ja | Ja |
| 33 | Bediensteter Elektronische Poststelle/Verwaltung | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Bediensteter Elektronische Poststelle/Verwaltung | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Bediensteter Elektronische Poststelle/Verwaltung | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Bediensteter Elektronische Poststelle/Verwaltung | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Bediensteter Elektronische Poststelle/Verwaltung | **weitere Funktionalitäten** | x | x | x | x | x |

Gewährte Funktionalitäten:

* Lesender Zugriff auf Leitdokument,
* Übermitteln des Postausgangs an Empfänger,
* Verwalten des zentralen Postein- und -ausgangs (Einsichtnahme, Weiterleitung, Übermittlung und Zurückweisung ggf. mit Begründung, Kennzeichnung als „gelesen“, „ungelesen“, „wichtig“, „Eilsache“),
* Weiterleiten des Einganges an Organisationseinheit/verantwortlichen Sachbearbeiter.

# Anlage 9 – Entitäten, Aktionsarten und Funktionalitäten des Bediensteten Geschäftsstelle

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Bediensteter Geschäftsstelle | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Bediensteter Geschäftsstelle | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Bediensteter Geschäftsstelle | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Bediensteter Geschäftsstelle | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Bediensteter Geschäftsstelle | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Bediensteter Geschäftsstelle | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Bediensteter Geschäftsstelle | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Bediensteter Geschäftsstelle | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Bediensteter Geschäftsstelle | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Bediensteter Geschäftsstelle | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Bediensteter Geschäftsstelle | **Berechtigungen** | Ja | Ja | Ja | Ja | Ja |
| 12 | Bediensteter Geschäftsstelle | **Posteingang OE** | Ja | Ja | x | Ja | Ja |
| 13 | Bediensteter Geschäftsstelle | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Bediensteter Geschäftsstelle | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | Bediensteter Geschäftsstelle | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | Bediensteter Geschäftsstelle | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Bediensteter Geschäftsstelle | **Verfahrenshistorie** | Ja | Nein | Nein | x | x |
| 18 | Bediensteter Geschäftsstelle | **Ordner** | Ja | Nein | Nein | x | x |
| 19 | Bediensteter Geschäftsstelle | **Unterordner im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 20 | Bediensteter Geschäftsstelle | **Dokumente im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 21 | Bediensteter Geschäftsstelle | **Kennzeichnung im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 22 | Bediensteter Geschäftsstelle | **Metadaten**  im Ordner „Akte“ | Ja | Nein | Nein | x | x |
| 23 | Bediensteter Geschäftsstelle | **Unterordner** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 24 | Bediensteter Geschäftsstelle | **Dokumente** in anderen Ordnern | Ja | Ja | Ja | x | x |
| 25 | Bediensteter Geschäftsstelle | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Ja | Ja | x | x |
| 26 | Bediensteter Geschäftsstelle | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | Bediensteter Geschäftsstelle | **Annotationen** | Ja | Nein | Nein | Nein | Nein |
| 28 | Bediensteter Geschäftsstelle | **Paginieren** | Ja | Nein | x | Nein | x |
| 29 | Bediensteter Geschäftsstelle | **Papierkorb** | Ja | Nein | Nein | x | x |
| 30 | Bediensteter Geschäftsstelle | **Repräsentat** | Ja | Nein | Nein | x | x |
| 31 | Bediensteter Geschäftsstelle | **Verfahrensabgabe** | Nein | Nein | Nein | Nein | Nein |
| 32 | Bediensteter Geschäftsstelle | **Workflow** | Ja | Ja | Ja | Ja | Ja |
| 33 | Bediensteter Geschäftsstelle | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Bediensteter Geschäftsstelle | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Bediensteter Geschäftsstelle | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Bediensteter Geschäftsstelle | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Bediensteter Geschäftsstelle | **weitere Funktionalitäten** | x | x | x | x | x |

# Anlage 10 – Entitäten, Aktionsarten und Funktionalitäten des Bediensteten Registratur

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Bediensteter Registratur | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Bediensteter Registratur | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Bediensteter Registratur | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Bediensteter Registratur | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Bediensteter Registratur | **Favoriten** | Ja | Ja | Ja | Ja | Ja |
| 6 | Bediensteter Registratur | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Bediensteter Registratur | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Bediensteter Registratur | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Bediensteter Registratur | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Bediensteter Registratur | **Rollen** | Nein | Nein | Nein | x | x |
| 11 | Bediensteter Registratur | **Berechtigungen** | Nein | Nein | Nein | Nein | Nein |
| 12 | Bediensteter Registratur | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | Bediensteter Registratur | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Bediensteter Registratur | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | Bediensteter Registratur | **Aktenführungsrecht** | Nein | Nein | Nein | Nein | x |
| 16 | Bediensteter Registratur | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Bediensteter Registratur | **Verfahrenshistorie** | Nein | Nein | Nein | x | x |
| 18 | Bediensteter Registratur | **Ordner** | Nein | Nein | Nein | x | x |
| 19 | Bediensteter Registratur | **Unterordner im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 20 | Bediensteter Registratur | **Dokumente im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 21 | Bediensteter Registratur | **Kennzeichnung im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 22 | Bediensteter Registratur | **Metadaten**  im Ordner „Akte“ | Nein | Nein | Nein | x | x |
| 23 | Bediensteter Registratur | **Unterordner** in anderen Ordnern | Nein | Nein | Nein | x | x |
| 24 | Bediensteter Registratur | **Dokumente** in anderen Ordnern | Nein | Nein | Nein | x | x |
| 25 | Bediensteter Registratur | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Nein | Nein | Nein | x | x |
| 26 | Bediensteter Registratur | **Templates** | Ja | Ja | Ja | Ja | Ja |
| 27 | Bediensteter Registratur | **Annotationen** | Nein | Nein | Nein | Nein | Nein |
| 28 | Bediensteter Registratur | **Paginieren** | Nein | Nein | x | Nein | x |
| 29 | Bediensteter Registratur | **Papierkorb** | Nein | Nein | Nein | x | x |
| 30 | Bediensteter Registratur | **Repräsentat** | Nein | Nein | Nein | x | x |
| 31 | Bediensteter Registratur | **Verfahrensabgabe** | Ja | Ja | Ja | Ja | Ja |
| 32 | Bediensteter Registratur | **Workflow** | Ja | Ja | Ja | Ja | Ja |
| 33 | Bediensteter Registratur | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Bediensteter Registratur | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Bediensteter Registratur | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Bediensteter Registratur | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Bediensteter Registratur | **weitere Funktionalitäten** | x | x | x | x | x |

# Anlage 11 – Entitäten, Aktionsarten und Funktionalitäten des beteiligten Sachbearbeiters Gastzugang

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Beteiligter Sachbearbeiter Gastzugang | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Beteiligter Sachbearbeiter Gastzugang | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Beteiligter Sachbearbeiter Gastzugang | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Beteiligter Sachbearbeiter Gastzugang | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Beteiligter Sachbearbeiter Gastzugang | **Favoriten** | Ja | Nein | Nein | Nein | Nein |
| 6 | Beteiligter Sachbearbeiter Gastzugang | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Beteiligter Sachbearbeiter Gastzugang | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Beteiligter Sachbearbeiter Gastzugang | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Beteiligter Sachbearbeiter Gastzugang | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Beteiligter Sachbearbeiter Gastzugang | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Beteiligter Sachbearbeiter Gastzugang | **Berechtigungen** | Ja | Nein | Nein | Nein | Nein |
| 12 | Beteiligter Sachbearbeiter Gastzugang | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | Beteiligter Sachbearbeiter Gastzugang | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Beteiligter Sachbearbeiter Gastzugang | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | Beteiligter Sachbearbeiter Gastzugang | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | Beteiligter Sachbearbeiter Gastzugang | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Beteiligter Sachbearbeiter Gastzugang | **Verfahrenshistorie** | Nein | Nein | Nein | x | x |
| 18 | Beteiligter Sachbearbeiter Gastzugang | **Ordner** | Ja | Nein | Nein | x | x |
| 19 | Beteiligter Sachbearbeiter Gastzugang | **Unterordner im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 20 | Beteiligter Sachbearbeiter Gastzugang | **Dokumente im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 21 | Beteiligter Sachbearbeiter Gastzugang | **Kennzeichnung im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 22 | Beteiligter Sachbearbeiter Gastzugang | **Metadaten**  im Ordner „Akte“ | Ja | Nein | Nein | x | x |
| 23 | Beteiligter Sachbearbeiter Gastzugang | **Unterordner** in anderen Ordnern | Ja | Nein | Nein | x | x |
| 24 | Beteiligter Sachbearbeiter Gastzugang | **Dokumente** in anderen Ordnern | Ja | Nein | Nein | x | x |
| 25 | Beteiligter Sachbearbeiter Gastzugang | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Nein | Nein | x | x |
| 26 | Beteiligter Sachbearbeiter Gastzugang | **Templates** | Ja | Nein | Nein | Nein | Nein |
| 27 | Beteiligter Sachbearbeiter Gastzugang | **Annotationen** | Ja | Nein | Nein | Nein | Nein |
| 28 | Beteiligter Sachbearbeiter Gastzugang | **Paginieren** | Ja | Nein | x | Nein | x |
| 29 | Beteiligter Sachbearbeiter Gastzugang | **Papierkorb** | Ja | Nein | Nein | x | x |
| 30 | Beteiligter Sachbearbeiter Gastzugang | **Repräsentat** | Ja | Nein | Nein | x | x |
| 31 | Beteiligter Sachbearbeiter Gastzugang | **Verfahrensabgabe** | Ja | Nein | Nein | Nein | Nein |
| 32 | Beteiligter Sachbearbeiter Gastzugang | **Workflow** | Ja | Nein | Nein | Nein | Nein |
| 33 | Beteiligter Sachbearbeiter Gastzugang | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Beteiligter Sachbearbeiter Gastzugang | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Beteiligter Sachbearbeiter Gastzugang | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Beteiligter Sachbearbeiter Gastzugang | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Beteiligter Sachbearbeiter Gastzugang | **weitere Funktionalitäten** | x | x | x | x | x |

# Anlage 12 – Entitäten, Aktionsarten und Funktionalitäten der Rechts- und Fachaufsicht

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Rechts-und Fachaufsicht | **Administrationsprotokollierung** | Nein | Nein | Nein | x | Nein |
| 2 | Rechts-und Fachaufsicht | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Rechts-und Fachaufsicht | **Statistik** | Ja | Nein | Nein | x | x |
| 4 | Rechts-und Fachaufsicht | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Rechts-und Fachaufsicht | **Favoriten** | Ja | Nein | Nein | Nein | Nein |
| 6 | Rechts-und Fachaufsicht | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Rechts-und Fachaufsicht | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Rechts-und Fachaufsicht | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Rechts-und Fachaufsicht | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Rechts-und Fachaufsicht | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Rechts-und Fachaufsicht | **Berechtigungen** | Ja | Nein | Nein | Nein | Nein |
| 12 | Rechts-und Fachaufsicht | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | Rechts-und Fachaufsicht | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Rechts-und Fachaufsicht | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | Rechts-und Fachaufsicht | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | Rechts-und Fachaufsicht | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Rechts-und Fachaufsicht | **Verfahrenshistorie** | Nein | Nein | Nein | x | x |
| 18 | Rechts-und Fachaufsicht | **Ordner** | Ja | Nein | Nein | x | x |
| 19 | Rechts-und Fachaufsicht | **Unterordner im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 20 | Rechts-und Fachaufsicht | **Dokumente im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 21 | Rechts-und Fachaufsicht | **Kennzeichnung im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 22 | Rechts-und Fachaufsicht | **Metadaten**  im Ordner „Akte“ | Ja | Nein | Nein | x | x |
| 23 | Rechts-und Fachaufsicht | **Unterordner** in anderen Ordnern | Ja | Nein | Nein | x | x |
| 24 | Rechts-und Fachaufsicht | **Dokumente** in anderen Ordnern | Ja | Nein | Nein | x | x |
| 25 | Rechts-und Fachaufsicht | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Nein | Nein | x | x |
| 26 | Rechts-und Fachaufsicht | **Templates** | Ja | Nein | Nein | Nein | Nein |
| 27 | Rechts-und Fachaufsicht | **Annotationen** | Ja | Nein | Nein | Nein | Nein |
| 28 | Rechts-und Fachaufsicht | **Paginieren** | Ja | Nein | x | Nein | x |
| 29 | Rechts-und Fachaufsicht | **Papierkorb** | Ja | Nein | Nein | x | x |
| 30 | Rechts-und Fachaufsicht | **Repräsentat** | Ja | Nein | Nein | x | x |
| 31 | Rechts-und Fachaufsicht | **Verfahrensabgabe** | Ja | Nein | Nein | Nein | Nein |
| 32 | Rechts-und Fachaufsicht | **Workflow** | Ja | Nein | Nein | Nein | Nein |
| 33 | Rechts-und Fachaufsicht | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Rechts-und Fachaufsicht | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Rechts-und Fachaufsicht | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Rechts-und Fachaufsicht | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Rechts-und Fachaufsicht | **weitere Funktionalitäten** | x | x | x | x | x |

# Anlage 13 – Entitäten, Aktionsarten und Funktionalitäten des Datenschutzbeauftragten

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Datenschutzbeauftragter | **Administrationsprotokollierung** | Ja | Nein | Nein | x | Nein |
| 2 | Datenschutzbeauftragter | **Fachdatenprotokollierung** | Ja | Nein | Nein | x | Nein |
| 3 | Datenschutzbeauftragter | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Datenschutzbeauftragter | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Datenschutzbeauftragter | **Favoriten** | Ja | Nein | Nein | Nein | Nein |
| 6 | Datenschutzbeauftragter | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Datenschutzbeauftragter | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Datenschutzbeauftragter | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Datenschutzbeauftragter | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Datenschutzbeauftragter | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Datenschutzbeauftragter | **Berechtigungen** | Ja | Nein | Nein | Nein | Nein |
| 12 | Datenschutzbeauftragter | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | Datenschutzbeauftragter | **Verfahren** | Ja | Nein | Nein | x | x |
| 14 | Datenschutzbeauftragter | **Bearbeitungsstatus** | Ja | Nein | x | x | x |
| 15 | Datenschutzbeauftragter | **Aktenführungsrecht** | Ja | Nein | Nein | Nein | x |
| 16 | Datenschutzbeauftragter | **Metadaten zum Verfahren** | Ja | Nein | Nein | x | x |
| 17 | Datenschutzbeauftragter | **Verfahrenshistorie** | Nein | Nein | Nein | x | x |
| 18 | Datenschutzbeauftragter | **Ordner** | Ja | Nein | Nein | x | x |
| 19 | Datenschutzbeauftragter | **Unterordner im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 20 | Datenschutzbeauftragter | **Dokumente im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 21 | Datenschutzbeauftragter | **Kennzeichnung im Ordner „Akte“** | Ja | Nein | Nein | x | x |
| 22 | Datenschutzbeauftragter | **Metadaten**  im Ordner „Akte“ | Ja | Nein | Nein | x | x |
| 23 | Datenschutzbeauftragter | **Unterordner** in anderen Ordnern | Ja | Nein | Nein | x | x |
| 24 | Datenschutzbeauftragter | **Dokumente** in anderen Ordnern | Ja | Nein | Nein | x | x |
| 25 | Datenschutzbeauftragter | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Ja | Nein | Nein | x | x |
| 26 | Datenschutzbeauftragter | **Templates** | Ja | Nein | Nein | Nein | Nein |
| 27 | Datenschutzbeauftragter | **Annotationen** | Ja | Nein | Nein | Nein | Nein |
| 28 | Datenschutzbeauftragter | **Paginieren** | Ja | Nein | x | Nein | x |
| 29 | Datenschutzbeauftragter | **Papierkorb** | Ja | Nein | Nein | x | x |
| 30 | Datenschutzbeauftragter | **Repräsentat** | Ja | Nein | Nein | x | x |
| 31 | Datenschutzbeauftragter | **Verfahrensabgabe** | Ja | Nein | Nein | Nein | Nein |
| 32 | Datenschutzbeauftragter | **Workflow** | Ja | Nein | Nein | Nein | Nein |
| 33 | Datenschutzbeauftragter | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Datenschutzbeauftragter | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Datenschutzbeauftragter | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Datenschutzbeauftragter | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Datenschutzbeauftragter | **weitere Funktionalitäten** | x | x | x | x | x |

# Anlage 14 – Entitäten, Aktionsarten und Funktionalitäten des Informationssicherheitsbeauftragten

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Rolle | **Aktionsart** | **Lesen/Öffnen** | **Schreiben** | **Löschen** | **Ausführen** | **Abbrechen** |
| **Entität/Funktionalitäten** |
| 1 | Informationssicherheitsbeauftragter | **Administrationsprotokollierung** | Ja | Nein | Nein | x | Nein |
| 2 | Informationssicherheitsbeauftragter | **Fachdatenprotokollierung** | Nein | Nein | Nein | x | Nein |
| 3 | Informationssicherheitsbeauftragter | **Statistik** | Nein | Nein | Nein | x | x |
| 4 | Informationssicherheitsbeauftragter | **Ansicht** | Ja | Ja | x | Ja | Ja |
| 5 | Informationssicherheitsbeauftragter | **Favoriten** | Ja | Nein | Nein | Nein | Nein |
| 6 | Informationssicherheitsbeauftragter | **Mandant** | Nein | Nein | Nein | x | x |
| 7 | Informationssicherheitsbeauftragter | **Dienststelle** | Ja | Nein | Nein | x | x |
| 8 | Informationssicherheitsbeauftragter | **Benutzergruppen der OE** | Ja | Nein | Nein | x | x |
| 9 | Informationssicherheitsbeauftragter | **Benutzer der OE** | Ja | Nein | Nein | x | x |
| 10 | Informationssicherheitsbeauftragter | **Rollen** | Ja | Nein | Nein | x | x |
| 11 | Informationssicherheitsbeauftragter | **Berechtigungen** | Ja | Nein | Nein | Nein | Nein |
| 12 | Informationssicherheitsbeauftragter | **Posteingang OE** | Nein | Nein | x | Nein | Nein |
| 13 | Informationssicherheitsbeauftragter | **Verfahren** | Nein | Nein | Nein | x | x |
| 14 | Informationssicherheitsbeauftragter | **Bearbeitungsstatus** | Nein | Nein | x | x | x |
| 15 | Informationssicherheitsbeauftragter | **Aktenführungsrecht** | Nein | Nein | Nein | Nein | x |
| 16 | Informationssicherheitsbeauftragter | **Metadaten zum Verfahren** | Nein | Nein | Nein | x | x |
| 17 | Informationssicherheitsbeauftragter | **Verfahrenshistorie** | Nein | Nein | Nein | x | x |
| 18 | Informationssicherheitsbeauftragter | **Ordner** | Nein | Nein | Nein | x | x |
| 19 | Informationssicherheitsbeauftragter | **Unterordner im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 20 | Informationssicherheitsbeauftragter | **Dokumente im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 21 | Informationssicherheitsbeauftragter | **Kennzeichnung im Ordner „Akte“** | Nein | Nein | Nein | x | x |
| 22 | Informationssicherheitsbeauftragter | **Metadaten**  im Ordner „Akte“ | Nein | Nein | Nein | x | x |
| 23 | Informationssicherheitsbeauftragter | **Unterordner** in anderen Ordnern | Nein | Nein | Nein | x | x |
| 24 | Informationssicherheitsbeauftragter | **Dokumente** in anderen Ordnern | Nein | Nein | Nein | x | x |
| 25 | Informationssicherheitsbeauftragter | **Metadaten** zu Unterordnern/ Dokumenten in anderen Ordnern | Nein | Nein | Nein | x | x |
| 26 | Informationssicherheitsbeauftragter | **Templates** | Nein | Nein | Nein | Nein | Nein |
| 27 | Informationssicherheitsbeauftragter | **Annotationen** | Nein | Nein | Nein | Nein | Nein |
| 28 | Informationssicherheitsbeauftragter | **Paginieren** | Nein | Nein | x | Nein | x |
| 29 | Informationssicherheitsbeauftragter | **Papierkorb** | Nein | Nein | Nein | x | x |
| 30 | Informationssicherheitsbeauftragter | **Repräsentat** | Nein | Nein | Nein | x | x |
| 31 | Informationssicherheitsbeauftragter | **Verfahrensabgabe** | Nein | Nein | Nein | Nein | Nein |
| 32 | Informationssicherheitsbeauftragter | **Workflow** | Nein | Nein | Nein | Nein | Nein |
| 33 | Informationssicherheitsbeauftragter | **Drucken** | Ja | Ja | x | Ja | Ja |
| 34 | Informationssicherheitsbeauftragter | **Kopieren** | Ja | Ja | x | Ja | Ja |
| 35 | Informationssicherheitsbeauftragter | **Verschieben** | Ja | Ja | x | Ja | Ja |
| 36 | Informationssicherheitsbeauftragter | **Wiederherstellen** | Ja | Ja | x | Ja | Ja |
| 37 | Informationssicherheitsbeauftragter | **weitere Funktionalitäten** | x | x | x | x | x |

1. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung unterschiedlicher geschlechtlicher Sprachformen verzichtet. Die Personenbezeichnungen gelten gleichwohl für sämtliche Geschlechter. [↑](#footnote-ref-1)
2. Dies umfasst alle Verfahren nach dem OWiG, einschließlich des Verwarnungsverfahrens. [↑](#footnote-ref-2)