KDN.sozial Fallmanagement für Jobcenter (kurz: FMG.job)

Benutzerprofilverwaltung und Rechtekonzept

Inhalt

Änderungshistorie

Datum	Seite	Änderung
16.10.2017	-	Erstellung des Verfahrenshinweises.
25.01.2017	6, 11	Jährliche Überprüfung definiert, Auflistung der MA mit Sonderrechten aktualisiert: Kristin Degener entfernt, Alexandra Hackenbroich ergänzt.
18.02.2019	11	Auflistung der MA mit Sonderrechten aktualisiert: Anette Ziegert entfernt.
14.06.2019	11	Auflistung der MA mit Sonderrechten aktualisiert: Norbert Hering ergänzt. Erweiterung um die Sonderrechte im Webdialog.
01.04.2020	-	Komplettaktualisierung und Auflistung der MA mit Sonderrechten aktualisiert: Im FMG2 Norbert Hering entfernt, Eva Pees, Alex Buick und Tanja Stüven ergänzt. Im Webdialog Lisa Schulz und Jan Wilke ergänzt.
18.11.2020	-	Auflistung der MA mit Sonderrechten aktualisiert: Im FMG2 Norbert Hering entfernt, Eva Pees, Alex Buick und Tanja Stüven ergänzt. Jonas Colsman, Oliver Hannig, Katharina Brauckmann, Barbara Grzechnik Zahlungsfreigabe entzogen. Dietrich Roscher entfernt. Peter Siegert, Andrea Szirmai Zahlungsfreigabe ergänzt. Im Webdialog Komplettüberprüfung. Änderung, dass Neuanlagen von Mitarbeiter*innen in KDN.sozial nicht mehr durch die IT erfolgen.
13.04.2021	-	Umfirmierung von AKDN sozial in KDN.sozial. Zurücksetzen von Benutzerkennungen ergänzt.
24.06.2021	12	Auflistung der MA mit Sonderrechten aktualisiert: Asiye Molla und Remi Teichmann entfernt; Rene Gerke ergänzt inkl. Zahlungsfreigabe 100.000 €.
21.07.2021	12	Auflistung der MA mit Sonderrechten aktualisiert: Dorothea Nowack ergänzt inkl. Zahlungsfreigabe 100.000 €.
31.05.2022	12	Umbenennung der Fachverfahren von FMG2 in FMG.job und Webdialog2 in Leistungsmanagement (LMG). Auflistung der MA mit Sonderrechten aktualisiert: Rene Gerke, Frank Mebus, Brigitte Rösner, Stefan Schulz, Michael Mosters Alexandra Sladojewic gelöscht. Maren Graßmann, Melanie Nohroudi, Kim Pupeter, Fabian Siepmann ergänzt mit Zahlungsfreigabe bis 2.000 €. Martin Dürholt, Ulrike Zechlin, Kathrin Hartmann, Dorothea Nowack, Justine Sigmundzik, Bianca Dörnemann ergänzt mit Zahlungsfreigabe 100.000 €. Tanja Stüven nur deaktiviert, damit Zahlungen noch ausgeführt werden können.
08.06.2022	12	Auflistung der MA mit Sonderrechten aktualisiert: Aysun Caliskan, Grischa Lamberti ergänzt mit Zahlungsfreigabe bis 2.000 €.
11.07.2022	6 ff.	Kapitelnummern korrigiert.
29.11.2022	14	Auflistung der Sonderrechte im LMG aktualisiert: Frau Schulz, Herrn Frahm, Frau Eligül entfernt. Herrn Stracke ergänzt.
01.06.2023	3	Ergänzung Verwendungshinweis
sämtliche Änderungen sind gelb hervorgehoben		

Verwendungshinweis

1. Ausgangslage

1.1 Organisatorische Anforderungen

Zur Gewährleistung der Anforderungen der internen und externen Revision sowie einer Funktionstrennung muss die Jobcenter Wuppertal AöR (JC) ein Konzept für die Benutzerverwaltung in KDN.sozial erstellen, welches mindestens die folgenden Punkte beinhaltet:

- Benutzer*innen dürfen sich nicht selbst verwalten
- die Verantwortlichkeiten für die Benutzerverwaltung müssen transparent sein
- die Nachvollziehbarkeit der Benutzerverwaltung muss sichergestellt werden

Dabei hat das JC einen begrenzten Personenkreis zu bestimmen, dem die Verwaltung von Benutzern*innen erlaubt ist. Die Benutzerverwaltung obliegt ausschließlich der jeweiligen KDN-Fachbetreuung aktiv wie passiv (siehe Organigramm).

Organigramm JBC_201808.pdf

Die Vertretung wird untereinander geregelt.

1.2 Benutzergruppen

Über Benutzergruppen wird bestimmt, für welche Bereiche ein*e Benutzer*in in KDN.sozial Zugriff erhält. Aus diesem Grund muss jede*r Benutzer*in einer Benutzergruppe zugeordnet werden. Diese bestimmt die entsprechenden Gruppenrechte. Die Gruppenrechte wiederum können in drei Kategorien unterteilt werden:

1. Zugriffsrechte auf einzelne Masken bzw. Reiter: Nur bei einem Teil der vorhandenen Benutzergruppen steht eine Gruppe für genau einen Reiter der Anwendung. In dem Fall kann gesteuert werden, welche dieser Reiter für einzelne Benutzer*innen ggf. gänzlich ausgeblendet werden. Sollen Masken allgemein gesperrt werden (z.B. der Reiter im FMG.job ***Kunden > Profiling***), wird dies in der TDSA-Verwaltung im Kreis-TDSA unter ***Einstellungen > gesperrte Masken*** vorgenommen. Die Masken können dann für einzelne Benutzer*innen über Schutzrechte wieder freigegeben werden.
2. Rechte zur Ausführung bestimmter Funktionen auf Masken bzw. Reitern
3. Rechte für unterschiedliche Benutzergruppen:
   - User*innen (***USR***)
   - Administratoren*innen (***ADM***)
   - Koordinatoren*innen (***KOR***)
   - Rechenzentrum-Administrator*innen (***RZADMIN***)

Die Vergabe mehrerer Benutzergruppen an die gleiche Benutzerkennung ist, abhängig von organisatorischen oder operativen Anforderungen, im Einzelfall zu prüfen.[1] In einem solchen Fall sollte ein*e

[1] z.B. Benutzer*innen mit Vollzugriff sowie Kostenfreigabe.

Benutzer*in auf Antrag zeitlich begrenzt mit einer separaten Kennung einer weiteren Benutzergruppe zugewiesen werden.

1.3 Entwicklungssysteme

Der Zugang zu den Entwicklungssystemen und den damit verbundenen Systemeinstellungen bleibt auf KDN.sozial bzw. die GKD Paderborn (Rechenzentrum der KDN.sozial) mit dem Gruppenrecht ***RZADMIN*** beschränkt. Ein weiterer Zugriff auf die KDN-Fachbetreuung bzw. die IT des JC wird nicht benötigt, da von dort keine Änderungen oder Anpassungen am System vorgenommen werden. Endanwender*innen wiederum dürfen gar keinen Zugang zum Entwicklungssystem erhalten.

Der Zugang zu einem Produktivsystem ist grundsätzlich nicht auf einen bestimmten Personenkreis eingeschränkt. Es müssen jedoch funktionale und organisatorische Einschränkungen entsprechend den definierten Aufgaben des*der Benutzers*in im Rahmen der Benutzerverwaltung vorgenommen werden.

1.4 Dokumentation

Die jeweilige KDN-Fachbetreuung ist zur Dokumentation aller möglichen Stufen eines Benutzerzyklus, wie etwa Anlage, Änderung oder Löschung von Benutzerkennungen oder Benutzerprofilen, verpflichtet. Hierzu ist das Dokument ***Änderungen-blanko.xlsx*** zu nutzen, das Antrag, Genehmigung und Art der Änderung entsprechend dokumentiert und archiviert. Es erfolgt je nach Fachanwendung eine eigenständige Dokumentation.

Änderungen-blanko.xlsx

2. Benutzerverwaltung

2.1 Anlage von Benutzerkennungen

Die jeweilige KDN-Fachbetreuung muss sicherstellen, dass nach dem "Prinzip der minimalen Berechtigung"[2] Benutzer*innen nur Zugriff auf diejenige Fachanwendung erhalten, die für die Ausübung seiner*ihrer Tätigkeit bzw. Funktion (Rolle) benötigt werden.

Für die Anlage von Benutzerkennungen ist seit 11/2020 ausschließlich die KDN-Fachbetreuung zuständig. Dabei müssen folgende Angaben gemacht werden:

- eine der Namenskonvention entsprechende Benutzerkennung (siehe Anlage 1)
  - Benutzerkennungen für Dialogbenutzer*innen müssen eindeutig sein
  - jede*r Benutzer*in darf nur über eine einzige, ihm*ihr zuordenbare, Benutzerkennung verfügen
  - für jede Benutzerkennung ist ein*e Verantwortliche*r festzulegen, auch wenn die Benutzerkennung nicht für eine interaktive Anmeldung verwendet wird

  Alle Benutzerkennungen müssen regelmäßig (einmal im Jahr) von der KDN-Fachbetreuung auf die Einhaltung der Namenskonventionen überprüft werden. Abweichungen von den Namenskonventionen sind zu klären und ggf. zu korrigieren.

[2] So wenig Berechtigungen wie möglich und nur so viele wie zwingend erforderlich.

- Stammdaten des*der Benutzers*in
- Vergabe des zukünftigen Benutzerprofils, das den Zugang zur Fachanwendung ermöglicht
- Vergabe des Aktenzeichens über die Teamzugehörigkeit

2.2 Zugang für externe Dritte

Der Zugang zu KDN.sozial ist für externe Dritte nicht vorgesehen, wird aber aktuell für das FMG.job in eingeschränkter Form geprüft. Der externe Zugriff obliegt derzeit alleine KDN.sozial selbst sowie der GKD Paderborn, die als Rechenzentrum die Betreuung und das Hosting von KDN.sozial für das JC gewährleistet.

2.3 Sperrung von Benutzerkennungen

Eine Benutzerkennung wird gesperrt bzw. deaktiviert, wenn folgende Voraussetzungen gegeben sind:

- Sperrung eines*er Benutzers*in aufgrund geänderter Personaldaten
- Sperrung aufgrund von (drei) Falschanmeldungen
- Sperrung, falls eine Benutzerkennung länger als 90 Tage nicht genutzt wurde

Die Sperrung der Benutzerkennungen erfolgt durch die jeweilige KDN-Fachbetreuung. Bei Unregelmäßigkeiten kann die Sperrung auch von der IT vorgenommen werden. Um den Betrieb des Systems nicht zu gefährden, gelten diese Regeln nicht für die folgenden Benutzer:

- Mitarbeiter*innen der GKD Paderborn
- Mitarbeiter*innen mit Vollzugriff

2.4 Entsperrung von Benutzerkennungen

Sofern eine Benutzerkennung gesperrt wurde, muss ein formloser Antrag (per E-Mail an das jeweilige Teampostfach) auf Entsperrung gestellt werden. Die KDN-Fachbetreuung überprüft die Identität des*der Benutzers*in. Sofern der*die Antragsteller*in als der*die Besitzer*in der Benutzerkennung identifiziert wurde, wird die Sperre aufgrund z.B. ungültiger Anmeldeversuche zurückgesetzt und bei Bedarf ein neues Initialkennwort erzeugt. Dieses wird an die E-Mail-Adresse, die in den Benutzerstammdaten enthalten ist, geschickt. In dieser E-Mail wird der*die Benutzer*in aufgefordert, das Initialkennwort umgehend zu ändern und über mögliche Folgen einer verzögerten Änderung informiert.[3]

Seit der FMG.job-Version 4.10 gibt es zudem die Möglichkeit, dass Benutzer*innen ihr Kennwort selber zurücksetzen können. Hierzu muss bei den eigenen Login-Daten eine 4-stellige PIN vergeben werden. Ferner muss in der Benutzerverwaltung zur Verifizierung eine E-Mail-Adresse hinterlegt sein. Nach einem Klick auf den Link "Kennwort zurücksetzen" auf der Login-Seite wird der*die Benutzer*in auf eine neue Seite umgeleitet, auf der der Login-Name und die E-Mail-Adresse eintragen werden müssen. Der*die Benutzer erhält damit eine E-Mail mit einem Link zugeschickt, worüber zur Sicherheit die hinterlegte PIN eingeben werden muss. War die Eingabe korrekt, wird dem*der Benutzer*in ein neu generiertes Initialkennwort in einer weiteren E-Mail zugeschickt.

[3] Textvorschlag: *"Bitte ändern Sie umgehend das Initialkennwort. Beachten Sie hierbei bitte die für KDN.sozial gültigen Kennwortregeln. Bei einer verzögerten Änderung des Initialkennworts sind Sie für alle Aktionen verantwortlich, die unter diesem Kennwort durchgeführt wurden."* Evtl. könnte man die Namenskonvention noch mit anführen.

2.5 Löschung von Benutzerkennungen

Benutzerkennungen werden nur aus der Fachanwendung gelöscht, wenn durch das Team Personal bestätigt wurde, dass der*die Benutzer*in nicht mehr beim JC arbeitet. Bevor jedoch eine Benutzerkennung aus einer Fachanwendung gelöscht wird, muss sichergestellt werden, dass

- eine Historie der Benutzerkennungen und der dazugehörigen Benutzer*innen, welche alle lokalen Anforderungen erfüllt, einen angemessenen Zeitraum zur Verfügung steht.[4]
- die Nachvollziehbarkeit der Systemvorgänge in den jeweiligen Fachanwendungen (wer hat was angelegt, geändert etc.) über einen bestimmten Zeitraum (in der Regel 10 Jahre) trotz Löschung der Benutzerkennung gewährleistet ist.

Diese Maßnahmen stellen die Transparenz, Nachvollziehbarkeit der eingesetzten Verfahren sowie die Einhaltung von Prüfungsanforderungen sicher.

Aus den TDSA-Gemeinden 107 und 131 dürfen allerdings wegen laufender Kassensätze keine Mitarbeiter*innen gelöscht werden. Andernfalls werden geplante Zahlungen nicht mehr ausgeführt. Eine Löschung dieser Mitarbeiter*innen kann erst erfolgen, wenn diese Zahlungen abschließend ausgeführt wurden. In solchen Fällen ist in der Benutzerverwaltung im Bemerkungsfeld das Datum der letzten Überprüfung einzugeben. Zudem erhalten sie ein eigenes Benutzerprofil.

2.6 Aktualität von Benutzerstammdaten

Team- und/oder Geschäftsstellenleitungen müssen die Aktualität der Benutzerstammdaten gewährleisten. Dies betrifft u.a. Änderungen von Funktionen oder Organisationsebenen des*der Benutzers*in, da dies zu Änderungen der Berechtigungen führen kann. Es ist die Aufgabe der Team- und/oder Geschäftsstellenleitung, zu dessen Organisationseinheit der*die Benutzer*in gehört, dafür zu sorgen, dass die Stammdaten, genauso wie die zugewiesenen Benutzerprofile, aktuell sind. Die Fachabteilungen haben eine jährliche Prüfung bis zum 31.12. eines Jahres zu gewährleisten und an die KDN-Fachbetreuung rückzumelden. Diese erstellen für diesen Zweck jeweils eine entsprechende Liste der in der Fachanwendung aufgeführten Mitarbeiter*innen und versenden diese zum 30.11. eines Jahres an die Team- und/oder Geschäftsstellenleitungen zur Prüfung.

Sobald ein*e Benutzer*in seine*ihre Organisationseinheit wechselt, ist die KDN-Fachbetreuung verpflichtet zu prüfen, ob die bislang vergebenen Berechtigungen noch benötigt und/oder innerhalb eines bestimmten Zeitraums entzogen/eingeschränkt werden müssen.

2.7 Technische Benutzerkennungen

Technische Benutzerkennungen (z.B. für virtuelle Mitarbeiter oder Pools für abgemeldete Kunden*innen etc.) müssen eindeutig von den Benutzerkennungen für "normale" Dialogbenutzer*innen unterschieden werden können. Dies muss durch

- eine entsprechende Namenskonvention,
- Benutzergruppen und
- Rollen

gewährleistet sein.

[4] Der Ausdruck der sog. Langliste aus KDN.sozial erfolgt einmal im Monat.

Für jede Benutzerkennung muss ein*e Verantwortliche*r definiert werden, auch wenn die betroffene Benutzerkennung nicht für eine interaktive Anmeldung verwendet wird. In der Regel übernimmt dies die jeweilige Teamleitung.

3. Berechtigungsverwaltung

3.1 Verwendung von Benutzerprofilen

Um Geschäftsdaten und -funktionen vor unberechtigten Zugriffen zu schützen, werden die verschiedenen Funktionen der jeweiligen Fachanwendung durch Berechtigungsprüfungen geschützt. Zugriffsberechtigungen werden dem*der Benutzer*in über Benutzerprofile, die in dem Benutzerdatensatz eingetragen wurden, zugewiesen.

3.2 Organisatorische Einschränkungen von Benutzerprofilen

Damit überprüft werden kann, welche Benutzer*innen eine Zugriffsberechtigung innerhalb einer Organisationseinheit haben, müssen ihre Rollen auf die einzelnen Bereiche beschränkt sein. Eine Unterteilung in verschiedene Organisationsebenen ist beim JC nicht vorgesehen. Zugriffsberechtigungen orientieren sich allein an der Rolle und dem damit zugewiesenen Benutzerprofil.

Die Ausübung von mehreren Rollen über verschiedene Geschäftsbereiche bzw. Abteilungen hinweg ist in KDN.sozial nicht möglich. Sollte ein solcher Fall notwendig sein, ist der*die Benutzer*in auf Antrag mit einer zweiten Kennung in der jeweiligen Fachanwendung anzulegen. Dadurch kann ihm*ihr dann ein anderes, zeitlich begrenztes Benutzerprofil zugewiesen werden (→ siehe Kapitel 3.4).

3.3 Benutzerprofilverwaltung

Alle Benutzerprofile müssen beschrieben und dokumentiert werden. Sie orientieren sich an der ausgeübten Tätigkeit und der entsprechenden Arbeitsplatzbeschreibung. Innerhalb einer Beschreibung müssen alle durch das jeweilige Profil zugänglichen Zugriffsberechtigungen definiert werden (→ siehe Kapitel 3.4).

Ein Benutzerprofil darf grundsätzlich keine Berechtigungen oder Berechtigungskombinationen enthalten, die durch die KDN-Fachbetreuung als kritisch oder als sensitiv definiert wurden, sofern dies von den Fachbereichsleitungen nicht explizit genehmigt wurde. Ein Benutzerprofil, das kritisch/sensitive Berechtigungen (bspw. Kostenfreigabe) enthält, wird automatisch als kritisch/sensitiv angesehen. Die KDN-Fachbetreuung muss solche Berechtigungen sowie die Zuordnung der Rollen in regelmäßigen Abständen überprüfen und entscheiden, ob diese immer noch benötigt werden. Ein Bericht über diese Überprüfung ist einmal im Jahr an die Innenrevision zu senden (siehe Anlage 2).

3.4 Anlage neuer Benutzerprofile

Jedem*er Mitarbeiter*in des JC ist entsprechend seiner*ihrer ausgeübten Tätigkeit einer Rolle zugewiesen, die sich aus dem Organigramm ableiten lässt. Gemäß der Rolle wird dem*der Benutzer*in in KDN.sozial ein Benutzerprofil zugewiesen.


Rechtekonzept KDN FMG2 20221019.xlsx


Rechtekonzept AKDN Webdialog 20171011

Der*die Vorgesetzte des*der Benutzers*in ist verantwortlich für die Überprüfung und Genehmigung des dokumentierten Benutzerantrags. Die Genehmigung eines Benutzerantrags muss mindestens einem "4-Augen-Prinzip" folgen:

- Im ersten Schritt muss jeder Antrag vom*von der Team- und/oder Geschäftsstellenleitung des*der Benutzers*in, welche*r für die Kontrolle und Genehmigung der dokumentierten Zugriffsanforderungen des Benutzers zuständig ist, geprüft und genehmigt werden.
- Die zweite Genehmigung muss von der KDN-Fachbetreuung des angeforderten Benutzerprofils durchgeführt werden. Für den Fall, dass Buchungskreisübergreifende Zugriffe (z.B. Zahlungsfreigaben) angefordert werden, müssen die Fachbereichsleitungen involviert werden.

Die Antragstellung auf Neuanlage eines Benutzerprofils von neuen Mitarbeiter*innen erfolgt automatisch durch den Informationsverteiler des Teams Personal (JBC.1101). Die KDN-Fachbetreuunng vergibt dann das zukünftige Benutzerprofil, das den Zugang zur Fachanwendung ermöglicht. Das sog. Starterprofil wird seit 11/2020 nicht mehr benötigt.

Bei der Anlage eines weiteren, neuen Bewerberprofils bzw. der Anlage eines technischen Mitarbeiters ist die Antragstellung schriftllich per E-Mail über die Team- bzw. Geschäftsstellenleitung zu erfolgen.

Die KDN-Fachbetreuung ist für als kritisch/sensitiv definierte Benutzerprofile verantwortlich und muss entsprechend am Genehmigungsprozess beteiligt werden, da sie die Zusammenhänge der beantragten Zugriffsrechte beurteilen muss. Erst wenn alle notwendigen Genehmigungen und alle Kontrollprozesse ausreichend dokumentiert sind, wird das Benutzerprofil der Benutzerkennung zugewiesen.

3.5 Änderung bestehender Benutzerprofile

Anträge für die Änderung einer Rolle müssen ebenfalls einem "4-Augen-Prinzip" folgen und orientieren sich an dem Verfahren der Neuanlage. Sofern die Änderung eines Benutzerprofils aufgrund bestimmter Geschäftsanforderungen notwendig ist, muss die zuständige KDN-Fachbetreuung den Änderungsprozess anstoßen. Hierbei müssen Funktionstrennung und kritisch/sensitive Berechtigungen berücksichtigt werden.

3.6 Löschung von Benutzerprofilen

Die Löschung von Benutzerprofilen aus einer der Fachanwendungen ist aus administrativen Gründen nicht vorgesehen. Ferner kann ein Benutzerprofil nur gelöscht werden, wenn es von keinem*er Benutzer*in mehr genutzt wird. Die Löschung eines Profils hat keine Auswirkungen auf die Nachvollziehbarkeit ihres Inhalts und die Zuordnung zu Benutzerkennungen, so dass eine Löschung auch die Anforderungen einer Revision erfüllt. Im Falle einer Löschung eines Benutzerprofils bleiben die damit vergebenen Rechte in jedem Fall erhalten.

3.7 Berechtigungen für besondere Projekte

Sobald ein Projekt definiert und genehmigt wurde, muss durch die Fachbereichsleitung und das Projektteam festgelegt und dokumentiert werden, welche notwendigen Zugriffsberechtigungen definiert werden müssen. Sie werden ebenfalls über ein Benutzerprofil gesteuert. Für diese Berechtigungen finden alle weiter oben gemachten Regeln und Prozesse Anwendung.

Ein solches Benutzerprofil darf nur an die festgelegten Mitglieder des Projektteams und nur für die Dauer des Projekts selbst vergeben werden. Nach Beendigung des Projektes ist das Benutzerprofil wieder zu löschen, und der Benutzer erhält gemäß seiner Rolle das dafür vorgesehene Profil wieder zurück.

4. Einsatz von Notfallbenutzern

Für Notfälle hat die GKD Paderborn als RZ-Admin Vollzugriff auf beide Fachanwendungen und kann bei Bedarf in die Zugriffsberechtigungen eingreifen.

Definition eines Notfalls:

- betrifft nicht den täglichen Betrieb
- kommt nicht periodisch vor
- betrifft kritische Systemkomponenten

Alle Anforderungen für die Verwendung einer Notfallbenutzerkennung müssen dokumentiert werden und müssen im Einzelfall mit der jeweiligen Fachbereichsleitung abgesprochen sein. Die Aktivitäten von Notfallbenutzern müssen systemseitig protokolliert werden. Die KDN-Fachbetreuung muss regelmäßig die Effektivität dieses Prozesses überwachen.

5. Funktionstrennung

Von der jeweiligen KDN-Fachbetreuung muss eine Liste von Zugriffsberechtigungen, die inkompatible Aufgaben und/oder Verantwortlichkeiten repräsentieren und nicht in einem Benutzerprofil gemeinsam vorkommen dürfen, definiert werden. Für die Erstellung einer solchen Liste werden die Anforderungen aus den Geschäftsprozessen berücksichtigt (siehe Anlage 2).

Die Funktionstrennung unterstützt dabei die Transparenz von Geschäftsprozessen zur Vermeidung von Unregelmäßigkeiten, Betrug und anderer strafbarer Tatbestände (dolose Handlungen). Aus diesem Grund muss bei jeder Rollenänderung oder bei der Zuweisung von Rollen zu Benutzerprofilen die Einhaltung der Funktionstrennung geprüft werden.

6. Kritisch/Sensitive Berechtigungen

Neben dem Problemkreis der Funktionstrennung können auch einzelne Zugriffsberechtigungen als kritisch oder sensitiv betrachtet werden. Eine Liste kritisch/sensitiver Berechtigungen muss mit den Fachbereichsleitungen definiert werden und ist dem jeweiligen Rechtekonzept zu entnehmen. Hierbei wird unterschieden nach:

- kritische Berechtigungen innerhalb eines Benutzerprofils für die Administration oder für Notfälle
- sensitive Berechtigungen innerhalb eines Benutzerprofils für spezielle Zwecke

Sofern Berechtigungen, die in diesen Kategorien aufgeführt sind, in Benutzerprofilen eingetragen werden sollen, müssen von der Innenrevision angemessene Maßnahmen für ein Risiko-Management eingeführt werden.

Verteiler

- Vorstand
- FBL FB 1-4
- Datenschutzbeauftragte
- Innenrevision
- Wirtschaftsprüfung IT

Anlage 1: Namenskonventionen für Benutzer*innen

1. Der Nachname plus der erste Buchstabe des Vornamens ist gleich Benutzername. Eine Umsetzung in Großbuchstaben erfolgt nicht. Der jeweils erste Buchstabe sollte großgeschrieben werden.
2. Die maximale Länge des Benutzers sollte 15 Stellen aus Gründen der Usability nicht überschreiten. Ist der Benutzername jedoch länger, wird nicht abgeschnitten.
3. Die folgenden Sonderzeichen sollten umgeschrieben werden: ä in ae, ö in oe, ü in ue, ß in ss. Auf typografische Sonderzeichen wie [,], {, }, ", ', <, >, | etc. ist zu verzichten.
4. Bei Doppelnamen sollte nur der erste Namen aufgenommen werden. Ggf. ist der*die Benutzer*in zu fragen, welcher Namensteil als Benutzername genommen werden soll.
5. Mehrfach vorkommende Namen sollten sich anhand des ersten Buchstabens des Vornamens unterscheiden. Ggf. ist auf den zweiten Buchstaben des Vornamens auszuweichen.
6. Sollte ein Benutzer eine zweite Benutzerkennung benötigen, ist eine fortlaufende Nummerierung zu nutzen.

Beispiele:

zu 1. Martina Mustermann = MustermannM
zu 2. Zarah Zimmermannundzimmerfrau = ZimmermannZ
zu 3. Zögling = Zoegling
zu 4. Bernd Regele-Umlauf = RegeleB
zu 5. Klaus Ahlborn = AhlbornKl
Karin Ahlborn = AhlbornKa
zu 6. Angela Ahlborn = AhlbornA und AhlbornA2

Anlage 2: Auflistung der Sonderrechte im FMG.job

Rolle	Name	Orga	Profil	Freibetrag
Fachbereichsleitung Leistung & Recht	Derzeit unbesetzt	JBC.2	VollZ+KF	100.000,00 €
Fachbereichsleitung Berufliche Integration	Herr Martin Dürholt	JBC.3	VollZ+KF	100.000,00 €
Fachreferentin Berufliche Integration	Frau Eva Pees	JBC.3001	VollZ+KF	100.000,00 €
Fachbetreuung KDN.sozial & DQM	Frau Natalie Dressler Herr Bernd Regele-Umlauf	JBC.0714	VollZ+KF+VIP	0,00 €
Leitung Maßnahmenmanagement	Frau Ulrike Zechlin (komm.)	JBC.31	MM-TL	100.000,00 €
Teamleitung Maßnahmenmanagement	derzeit unbesetzt	JBC.31	MM-TL	100.000,00 €
Sachbearbeitung Maßnahmemanagement g.D. mit Freigabe	Herr Stephan Bäcker Herr Uwe Graf Frau Kathrin Hartmann Frau Dorothea Nowack Herr Sven Schagen Herr Peter Siegert Frau Justine Sigmundzik Frau Andrea Szirmai Herr Frank Mebus	JBC.3101	MM-Experte	100.000,00 €
Sachbearbeitung Maßnahmemanagement m.D. mit Freigabe	Frau Maren Graßmann Frau Melanie Nohroudi Frau Kim Pupeter Herr Fabian Siepmann Frau Aysun Caliskan Herr Grischa Lamberti	JBC.3102	MM-Experte	2.000,00 €
Fachreferent*in Maßnahmenmanagement	Frau Simone Gall Frau Alex Buick	JBC.3101	MM-Experte	100.000,00 €
Vorstandsbüro & Beschwerdemanagement	Frau Bianca Dörnemann	JBC.02	Führung	0,00 €
Urlaubs- & Krankheitswesen	Frau Heike Branca	JBC.1104	Führung	0,00 €

Anlage 3: Auflistung der Sonderrechte im LMG

Team	Name	Profil + zusätzliche Rechte
	Herr Stelzer	Rechte LG und FR + 15.000 € Freigabe im Ez-Verfahren, Export CSV
3220	Herr Kastien	Rechte LG und FR + 99.000 € Freigabe im Ez-Verfahren, Export CSV
24	Frau Bentler	Rückforderung+AZR
324	Frau Zechlin	Geschäftststellenleiterin + Zeugenschutz
2001	Herr Dornseif	Führungsunterstützung + AZR + Experte
2001	**Frau Schulz**	Führungsunterstützung + AZR + Experte
3142	Frau Heringer	Lesend+ Zeugenschutz
3242	Frau Braun	Teamleiter + Zeugenschutz
3242	Frau Ryglewski	Expertin + Zeugenschutz+AZR
3249	Herr Hering	Teamleitung + Mitarbeiterakte
3249	Herr Bornhuse	Experte + Mitarbeiterakte
3249	**Herr Frahm**	Experte + Mitarbeiterakte
3249	Herr Spieß	Experte + Mitarbeiterakte
4850	Herr Grawe	Fachreferat Recht+AZR+Experte
4850	**Frau Eligül**	Teamleitung+AZR
4850	Herr Ferdyan	Fachreferat Recht+AZR+LG gehobener Dienst
4850	Herr Wilke	Fachreferat Recht+AZR+Experte
4850	Frau Mühlbeier	Fachreferat Recht+AZR+Experte - Antrag Frau Schulz vom 15.12.2020 per Mail
4854	Herr Stracke	studentische Hilfskräfte für die Antragsaufnahme Ukraine – Ursprungsprofil Einarbeitung aber nur für Raten 71-79 Zebera