Vortrag im AK IV-Rev. EVU
Wiesbaden 2024

Datenschutz in SAP HCM

„P_PERNR, P_ORGIN, P_ORGXX

Seit wann sind die Infotypen 0008 und 0015 eindeutig schützenswerte Beschäftigtendaten? Und was bedeutet das?“

C. Wildensee

Einleitung und Rechtsgrundlagen / Problemdarstellung

Grundsätzlich gibt es keinen allgemeingültigen Katalog personenbezogener Daten der (elektronischen) Personalakte, der regelt, welche davon schützenswert sind (Ausnahme nach Art. 9 DSGVO) und welche davon wie genau welchen besonderen Schutz genießen.

Selbstverständlich gibt es eine Vielzahl an Gesetzen, wie mit verschiedenen Daten umzugehen ist, welche Anspruchsberechtigte vorhanden sind und welche Daten an externe Berechtigte in welcher Form zu fließen haben.

Welche Funktionen im Unternehmen welche Einsichts- und Manipulationsrechte auf personenbezogene Daten aufweisen, ist jedoch nicht abschließend geregelt.
ABER: Es gibt mit Wirkung seit 2019 eine rechtliche Klarstellung, die hier Signalwirkung entfaltet.

a) DSGVO (anzuwenden ab 2018, bekannt)	Zugriff durch Berechtigte+Gesetz
b) Entgelttransparenzgesetz+AGG (seit 2017+2006)	Zugriff des Betriebsrats in Vertr.
c) BAG-Beschlüsse aus 2019 und 2020	individuelle Gehältersicht im BR

BAG-Beschluss vom **7. Mai 2019** (Az. 1 ABR 53/17)

Leitsatz:

Die Berechtigung des **Betriebsausschusses oder** eines nach § 28 BetrVG **gebildeten Ausschusses** gemäß § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG, **in die Listen über die Bruttolöhne und -gehälter Einblick zu nehmen**, ist nicht auf anonymisierte Listen beschränkt.
[…]
„Der für das Einblicksrecht in die Listen über die Bruttolöhne und -gehälter nach § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG notwendige Aufgabenbezug ist regelmäßig schon deshalb gegeben, weil der Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG darüber zu wachen hat, dass die zugunsten der Arbeitnehmer geltenden Gesetze und Tarifverträge durchgeführt werden. Hierzu gehört auch die sich aus § 75 Abs. 1 BetrVG ergebende Verpflichtung des Arbeitgebers zur Beachtung des allgemeinen Gleichbehandlungsgrundsatzes. Der Darlegung eines besonderen Anlasses für die Ausübung dieses Einsichtsrechts bedarf es nicht (vgl. BAG 14. Januar 2014 - 1 ABR 54/12 - Rn. 23). Der Betriebsrat benötigt die Kenntnis der effektiv gezahlten Vergütungen, um sich ein Urteil darüber bilden zu können, ob insoweit ein Zustand innerbetrieblicher Lohngerechtigkeit existiert oder nur durch eine andere betriebliche Lohngestaltung erreicht werden kann. Ein Einsichtsrecht besteht deshalb auch dann, wenn der Betriebsrat gerade feststellen will, welche Arbeitnehmer Sonderzahlungen erhalten und wie hoch diese sind. Die Grenzen des Einsichtsrechts liegen dort, wo ein Beteiligungsrecht oder eine sonstige Aufgabe offensichtlich nicht in Betracht kommt (BAG 14. Januar 2014 - 1 ABR 54/12 - Rn. 23)“.
[…]

ABER: Limitierung durch **BAG-Beschluss vom 28. Juli 2020, Az: 1 ABR 6/19**: Daten in auswertbarem Format nur, wenn der Betriebsrat auch die Auskunftsersuchen der berechtigten Personen beantwortet. Erfolgt dies über den Personalbereich, müssen dem BR die Daten **nicht in auswertbarem Format** zur Verfügung gestellt werden. § 13 Abs. 2 EntgTranspG greift dann nicht. Ein Permanent-Sichtrecht für den BR ist nicht ableitbar, auch nicht aus dem Grund der Administrationsvereinfachung.

Rechtssicht in der Prüfung (1/3)

Die **BAG-Beschlüsse haben Signalwirkung** und entfalten nachvollziehbar diese Sicht:

- Beschäftigtendaten unterliegen dem Datenschutzrecht (siehe Art. 6 DSGVO), eine Verarbeitung und Permanent-Einsicht ist nur zulässig zur Durchführung des Vertrags und der sich daraus ergebenden Sekundärpflichten (ESt, KV, RV usw.), bei Vorliegen einer expliziten Einwilligung oder wenn ein konkretisierendes Gesetz darüber hinaus eine Rechtsgrundlage schafft. Die Verarbeitung unterliegt immer einer Zweckbindung.
- Grundsätzlich kann auch eine Interessenabwägung mit Datenschutzfolgeabschätzung (als rechtlich schwächste Möglichkeit) im Datenschutzrecht als Grundlage für die Einsicht dienen. Hier haben aber die BAG-Beschlüsse einen stark restriktiven Aspekt beigesteuert.
- Diese zeigen, dass sogar der Betriebsrat begrenzt ist in einem Permanent-Sichtrecht auf Gehaltsdaten der Beschäftigten und nur aufgrund einer gesetzlichen Grundlage & Aufgabe überhaupt Zugriff erhalten darf. Die Grundlage aus § 80 BetrVG ist zwingend.
- Permanent-Sichtrechte gehören also in keinen anderen Bereich außerhalb der Personalsachbearbeitung/-abrechnung und des Betriebsrats, sofern nicht eine Rechtsgrundlage oder individuelle Einwilligung eine explizite Ermächtigung erteilt.

(Sichtrecht als geringste Form des Zugriffs. Kenntnisnahme ist jedoch bereits nach DSGVO kritisch.)

Rechtssicht in der Prüfung (2/3)

Dies führt folglich zu folgenden Punkten:

- Sicht- und Manipulationsrechte auf indiv. Beschäftigtendaten und Gehaltsdaten im Unternehmen gehören in die Personalabteilung (Referentensicht) und Personal-abrechnung (auch ADV-Dienstleister aus Art. 28 i.V.m. 4 DSGVO). INFTY => 0008/0015
- Sichtrechte können auch in den Betriebsrat gehören => Betriebsratsmitglieder des Betriebsausschusses oder anderer Explizit-Ausschuss, nicht darüber hinausgehend.
- Art. 9-Daten im Abrechnungsbeleg? => ja! Vorsichtig bei 0004 (Behd.), 0057 (Mitgl.)…
- Ad-hoc-Rechte des Vorstands bzw. der Geschäftsführung aus deren Verpflichtung zur Überwachung des Unternehmens bleiben hiervon unberührt. Administration gilt nicht als Sicht-Ermächtigungstatbestand. Ist zu reduzieren, auch für Basisrechte (S-Objekte)
- Absicherungen sind ferner gem. Art. 25 und 32 DSGVO nach dem neuesten Stand der Technik zu gestalten. Zu beachten: Art. 9 bei Gehaltsbeleg => auch S_RFC eingrenzen
- Ein Nachvollzug der Rechtevergabe gem. Art. 5 Abs. 1f und Abs. 2 DSGVO insbesondere i.V.m. den Erwägungsgründen 39 und 74 ist zwingend.

(Die Systemadministration hat keine Rechtsgrundlage für den Zugriff auf individuelle Gehaltsbestandteile Beschäftigter!)

Rechtssicht in der Prüfung (3/3) => abschießend

- Wenn selbst der Betriebsrat trotz starker Rechtsgrundlage in seinem Sichtrecht auf Gehaltsdaten stark limitiert wird und ihn das Unternehmen daran hindern kann, überhaupt ein dauerhaftes Recht auf Einsicht zu erhalten und ausüben zu können, können alle anderen Bereiche des Unternehmens außerhalb des HR-Bereiches (dieser als zentraler HR-Dienstleister) keine Legitimation auf Einsicht ableiten – außer per expliziter Gesetzesgrundlage oder individueller Einwilligung (z.B. betr. Soz.beratung).
- Insbesondere der BAG-Beschluss aus 2020 zeigt ein Dilemma. Wer legt im Unternehmen fest, dass der Betriebsrat und nicht die Personalabteilung die zugrunde liegenden Auskunftsersuchen Berechtigter beantwortet? Das Ziel war eine Konkretisierung des Entgelttransparenzgesetzes zugunsten des Betriebsrates. Tatsächlich hat die Klarstellung des BAG eine mögliche Zwangslage und Eskalationsspirale zwischen Betriebsrat und Unternehmen geschaffen.
- In wohlwollender Abstimmung zwischen Betriebsrat und Unternehmen kann man aber ableiten, dass der Betriebsrat ein Permanent-Sichtrecht eingeräumt bekommen **kann**. Dies hilft bei der Erfüllung seiner Aufgaben und reduziert Eskalationspotential und administrativen Aufwand. Umfangsklärung aber über Personal- & Rechtsbereich.

Was bedeutet das in der Prüfung?

SAP HCM

Prüfungsschritte

1. Sichtrecht auf die Infotypen 0008 und 0015 für Personen außerhalb der eigenen Person erkennen

Dies betrifft die Berechtigungsobjekte P_ORGIN und P_PERNR. Ergänzend kommt für eine Vielzahl von Unternehmen die Steuerungsoption aus dem Objekt P_ORGXX hinzu (erweiterte Berechtigungsprüfung; T77S0 → AUTSW → ORGXX → 1).

2. Ausgehend von der Tabelle USOBT müssen die Transaktionsebene und alle übrigen, notwendigen Objektausprägungen einbezogen werden, die benötigt werden für PA20 (Personalstammdaten anzeigen).

Während in vielen SAP-Bereichen ein fehlendes Recht zum Transaktionsaufruf im Benutzerstammsatz substituiert werden kann durch Transaktionen wie z.B. SA38, OODR, START_REPORT oder ähnliche und der Angabe des hinter der gewünschten Transaktion stehenden Programmnamens, funktioniert diese Vorgehensweise für die Transaktionen PA20 (…anzeigen) und PA30 (…pflegen) nicht. **Insoweit muss eine der beiden Transaktionen in privilegierten Stammsätzen vorkommen, was wiederum eine wesentliche Funktion zur Separierung der Rechte darstellt.**

Zeigt die vollständige Sicht am Ende als Ergebnis, welche Stammsätze und daraus, welche Bereiche Zugriff erhalten, ist üblicherweise auch die Frage nach der adäquaten Steuerung beantwortet.

Was bedeutet das in der Prüfung?

Prüfungsschritte

3. Sofern wir annehmen, dass das Sichtrecht auf die Infotypen 0008 und 0015 bei anderen Personen als wesentliche Identifier der Rollenwahrnehmung und -trennung und die Transaktion PA20 ebenfalls hierzu diesen kann, bestehen mehrere Schritte zur Eingrenzung der Rollen und Berechtigungen.

- **Schritt A** besteht darin, die wesentlichen Arbeitsplatzrollen und deren Zuweisung zu den Stammsätzen zu identifizieren.

  Tabelle AGR_USERS: Innerhalb dieser Tabelle stehen sowohl die Einzel- als auch die Arbeitsplatz- / Sammelrollen, die den UserIDs / Stammsätzen mit Gültigkeitsbeginn und -ende zugewiesen sind. Eine Eingrenzung muss sowohl bezüglich der Namensgebung aus der Konvention heraus **auf Sammelrollen** als auch über FROM_DAT und TO_DAT erfolgen. Sinnvoll ist hier z.B., dass bei TO_DAT ein Datum größer voraussichtliches Prüfungsbeendigungsdatum gewählt wird, da ansonsten die Ergebnisse eine eingeschränkte Aktualität aufweisen können. Zunächst steht für dauerhaft beschäftigte Personen im Feld TO_DAT der 31.12.9999. Bei der Bedeutung der Rollen hilft die Einsicht in die Tabelle AGR_DEFINE mit den Feldnamen AGR_NAME und TEXT. **Access-DB => Kreuztabelle**

Ergebnis: Verteilung der Rollen auf die UserIDs, Rollen horizontal, UserIDs vertikal.

Was bedeutet das in der Prüfung?

Prüfungsschritte

- Jetzt haben wir eine qualifizierte Rollen-User-Liste, die weitere Inhalte aufnehmen kann. Notwendig ist an dieser Stelle, dass die organisatorische Zuweisung der UserIDs hinzugefügt wird, um Bereichs-gruppierungen ableiten zu können. Hierzu dient im **Schritt B** die Tabelle USER_ADDR, die Felder „Vollständiger Name“ und „Abteilung“ (Department) sind von großem Vorteil, um die korrekte Bereichszuweisung erkennen und hiernach sortieren zu können.

- **Schritt C**: Sofern eine Einzelrolle eine Eingrenzung des Objektes **P_PERNR** mit **PSIGN=E oder *** in der Tabelle AGR_1251 aufweist (Ausschluss = I), kann eine Arbeitsplatzrolle mit einer solchen zugewiesenen Einzelrolle auf Personalnummern zugreifen, die nicht die eigene ist (Zugriff auf die eigene Personalnummer ist für den „Employee Self Service“ [ESS] notwendig, insoweit wird es üblicherweise im Stammsatz ein P_PERNR mit PSIGN=I geben). Erhält man nun eine Liste der Einzelrollen, die P_PERNR im Feld PSIGN=E oder * (nicht I) aufweisen, müssen diese Einzelrollen auf Infotyp 0008 und 0015 überprüft werden. Werden diese in der Tabelle AGR_AGRS als Child geprüft, können die relevanten Arbeitsplatzrollen identifiziert und die Kreuztabelle sinnvoll reduziert werden. Es erfolgt die Prüfung des Objektes **P_ORGIN** auf Infotyp 0008 und 0015 in diesen Rollen. Subtyp-Eingrenzung ist zu beachten.
  (Personalbereiche = T500P; Personalbereiche = T501; Mitarbeiterkreis = T503K)

Ergebnis: Liste der Sammelrollen, die für die Gesamtsicht relevant sind. Eingrenzung der Sammelrollenliste und Personen, die diese aufweisen.

Was bedeutet das in der Prüfung?

Prüfungsschritte

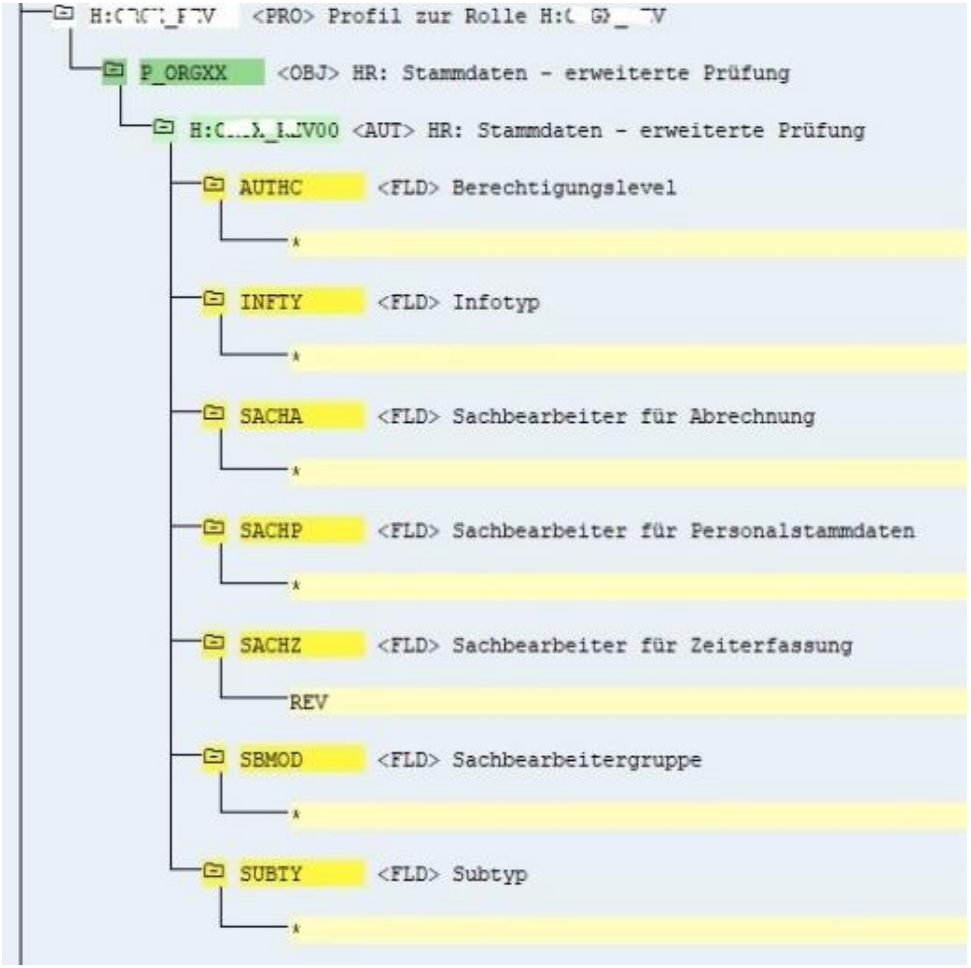
4. Erweiterte Berechtigungsprüfung (P_ORGXX)

Beispiel: Erhält ein/e Mitarbeiter/in die Fachbereichsfunktion **für die zeitwirtschaftliche Aufgaben** des Bereiches und hat über eine weitere Rolle Zugriff über P_ORGIN auf INFTY 0008/0015 und die Transaktion PA20 inkl. aller für diese Transaktion notwendigen, weiteren Ausprägungen, greift zusätzlich P_ORGXX aus der erweiterten Berechtigungsprüfung im Stammsatz, wenn zu der Funktion ein Profil hinterlegt ist und dieses eine zusätzliche Prüfung aufweist. Ist in dieser Prüfung dann ein begrenzendes Ordnungskriterium hinterlegt, erhält die Person mit PA20 nur Zugriff auf die Personen, die diesem Ordnungskriterium entsprechen. Dies gilt an der Stelle für alle Infotypen.

Für einige Arbeitsplatzfunktionen werden jeweils Profile angelegt, die beim Check des Zugriffes greifen, sofern sie dann zur UserID in Tabelle T77UA (UNAME, PROFL, BEGDA, ENDDA; Erläuterungen hierzu in Tabelle T77PQ) hinterlegt sind. Ist hier kein Profil für eine UserID hinterlegt und privilegierte Objektausprägungen sind für sie im Stammsatz vorliegend, gibt es nur aus diesen die Einschränkungen, die Person hat aber auf privilegiert hinterlegte Infotypen aller Beschäftigten (mindestens lesenden) Zugriff.

Was bedeutet das in der Prüfung?

Spannende Ergänzung

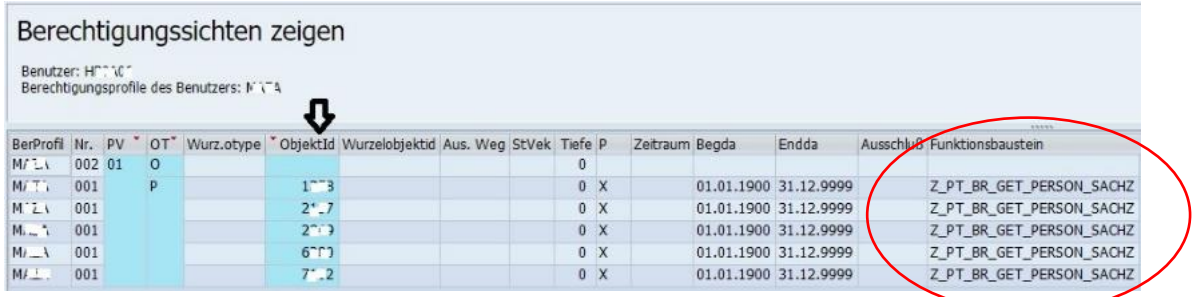


Die Person im Beispiel kann also nicht auf alle Beschäftigten des Unternehmens mit PA20 zugreifen, sondern nur auf die Personen, die dem Ordnungskriterium REV entsprechen (INFTY und alle anderen Felder bei P_ORGXX = *), dort allerdings auf alle Infotypen (Subtyp = *), die unter dem Objekt P_ORGIN angegeben wurden. Auch wenn ein zweites P_ORGXX im Stammsatz vorhanden ist, sucht sich (dies ist ein Unterschied zu SAP Core, hier zählt die höchste Ausprägung im Stammsatz) SAP HCM die Objektausprägung, die mit dem Profil eine Eingrenzung aufweist. Ist dies der Fall, wird auf die Eingrenzung reduziert. Im Beispiel ist die Referenz der pflegenden Personen zum Ordnungskriterium SACHZ in Tabelle T526 zu finden (SACHX, SACHN und USRID).

Was bedeutet das in der Prüfung?

Wie erfolgt die Steuerung?

In der Transaktion OOSB (Benutzer strukturelle Berechtigung) findet sich jeweils je UserID, die z.B. zeitwirtschaftlichen Aufgaben übernimmt, ein Eintrag mit einem Profil-Namen und einer Gültigkeit.



Lässt man sich die Objekte hierzu zur Person anzeigen, so zeigt sich, dass hier die Personalnummern eingetragen sind, für die diese Person tatsächlich die Aufgabe übernimmt. Eine Person aus einem anderen Bereich kann dann in der Sachbearbeitung der zeitwirtschaftlichen Aufgaben nicht ausgewählt werden, es werden nur die hier enthaltenen Personen in Gültigkeit angezeigt, die unter ObjektId mit der Personalnummer stehen.

Zum Profil wird der Ablauf aus dem Funktionsbaustein Z_PT_BR_GET_PERSON_SACHZ mitgegeben, der eine Prüfung auf das Feld PA0001-SACHZ durchläuft (FuBa hinterlegt zum Profil der Funktion des Mitarbeiters mit zeitwirtschaftlichen Aufgaben in Tabelle T77PR; Felder PROFL, LFDNR, PLVAR, OTYPE [=P] und PFUNC).

Was bedeutet das in der Prüfung?

Es ist also im **Schritt D** hier wichtig, zuletzt zu den UserIDs mit zeitwirtschaftlichen Aufgaben in der Kreuztabelle / Ergebnisliste die jeweils zugewiesenen Ordnungskriterien hinzuzufügen, um abschätzen zu können, ob die Zugriffe auf alle Beschäftigten des Hauses oder nur auf eine stark begrenzte Gruppe zutreffen und ggf. auch mit weiteren, hoch privilegierten Rechten kombiniert werden. Gleiches gilt für Planer.

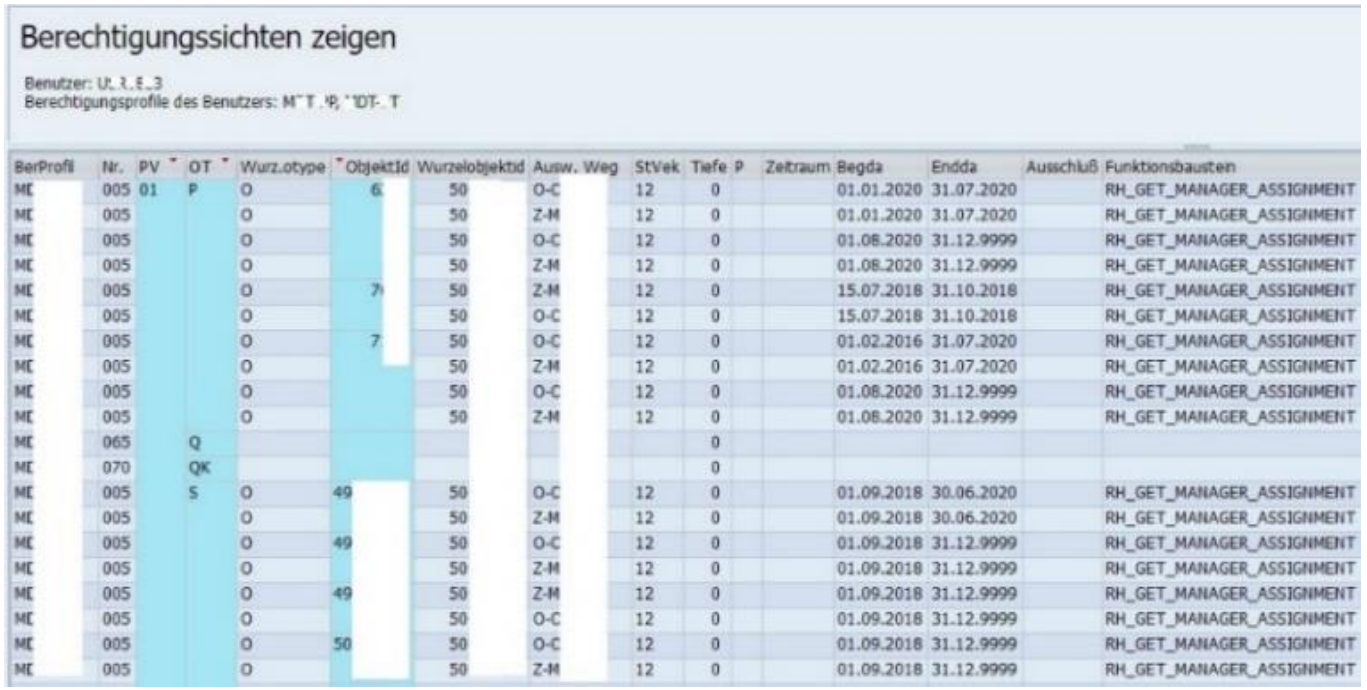
Beschäftigte des Personalbereichs weisen wiederum keine Profile auf, da sie auf alle Beschäftigten des Unternehmens Zugriff erhalten. Zur Übersicht ist hier die Bereichsgruppierung relevant. Sofern Zuständigkeitsaufteilungen innerhalb der Personalbearbeitung notwendig sind, wird hier analog verfahren.

Leitungsfunktion

Ähnlich ist auch die Steuerung des Managers Desktop (MD) für Führungskräfte. Es wird allerdings die **WurzelobjektID** als Basis in OOSB genutzt. Hier steht die Stellennummer der Führungskraft. Unter ObjektId stehen die Personalnummern (Objekttyp P) und die Stellennummern (Objekttyp S) der zugewiesenen Personen. Die Stellennummer der WurzelobjektID wird auch in der Tabelle T527X zur jeweiligen Bereichskennung gehalten (ORGEH, BEGDA, ENDDA und ORGTX). Zu den Profilen des Managers Desktop in T77UA gibt es in T77PR aber keine Funktionseinträge, die Prüfungen auf Referenzfelder beinhalten, da dies über die Hinterlegung der Auswertungswege nach T778A ausreicht (Referenz auf SAP-FuBa RH_GET_... [siehe nächste Folie]). In vielen Unternehmen läuft dieses Procedere annähernd wie dargestellt. Die FuBa-Namen und Prüfungsobjekte sind dann aber abweichend.

Was bedeutet das in der Prüfung?

Führungskräfte



Berechtigungssichten zeigen

Benutzer: U. ?. E_3
Berechtigungsprofile des Benutzers: M T .P; IDT- T

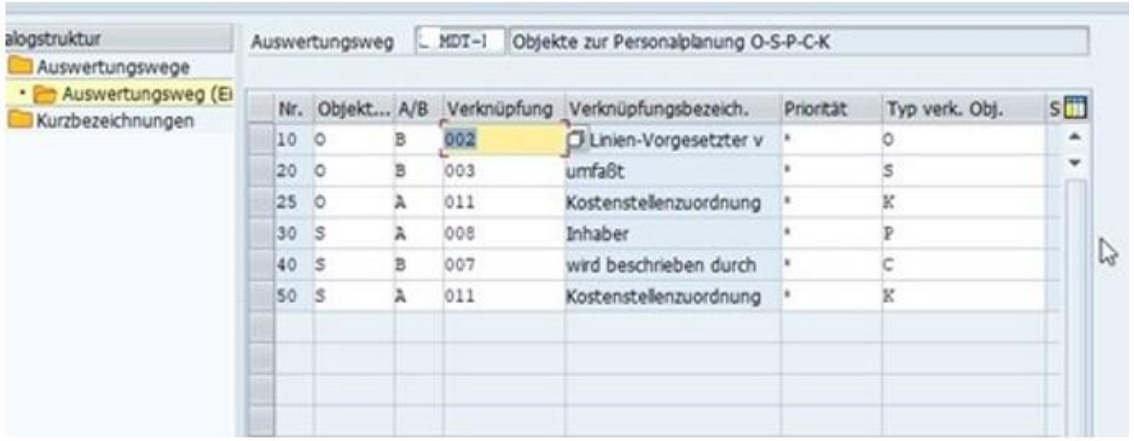
BerProfil	Nr.	PV	OT	Wurz.otype	ObjektId	Wurzelobjektid	Ausw. Weg	StVek	Tiefe	P	Zeitraum	Begda	Endda	Ausschluß	Funktionsbausten
ME	005	01	P	O	6	50	O-C	12	0			01.01.2020	31.07.2020		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	Z-M	12	0			01.01.2020	31.07.2020		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	O-C	12	0			01.08.2020	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	Z-M	12	0			01.08.2020	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O	7	50	Z-M	12	0			15.07.2018	31.10.2018		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	O-C	12	0			15.07.2018	31.10.2018		RH_GET_MANAGER_ASSIGNMENT
ME	005			O	7	50	O-C	12	0			01.02.2016	31.07.2020		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	Z-M	12	0			01.02.2016	31.07.2020		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	O-C	12	0			01.08.2020	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	Z-M	12	0			01.08.2020	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	065		Q						0						
ME	070		QK						0						
ME	005		S	O	49	50	O-C	12	0			01.09.2018	30.06.2020		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	Z-M	12	0			01.09.2018	30.06.2020		RH_GET_MANAGER_ASSIGNMENT
ME	005			O	49	50	O-C	12	0			01.09.2018	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	Z-M	12	0			01.09.2018	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O	49	50	Z-M	12	0			01.09.2018	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	O-C	12	0			01.09.2018	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O	50	50	O-C	12	0			01.09.2018	31.12.9999		RH_GET_MANAGER_ASSIGNMENT
ME	005			O		50	Z-M	12	0			01.09.2018	31.12.9999		RH_GET_MANAGER_ASSIGNMENT

WurzelbjektID = Personalnummer Chef
ObjektID = Stellennummern und Personal-nummern der zugewiesenen Beschäftigten

Was bedeutet das in der Prüfung?

Führungskräfte

Im Bereich der Rechte auf Managers Desktop weist jede Führungskraft unter T77UA also ein oder mehrere MD-Profile auf, die wiederum keine weitere Eingrenzung aus P_ORGXX benötigen, da der Stellenplan greift, keine Einträge in T77PR vorliegen und sich die MD-Rechte nur auf Personen beziehen, die in der Hierarchiedarstellung analog der Verknüpfung zugeordnet sind.



01.09.2018	31.12.9999	A	012	leitet...	O	5006
01.02.2021	31.12.9999	B	002	ist Linien	S	6000
01.07.2018	31.12.9999	B	002	ist Linien	S	5006

Andere Profile können jedoch ebenfalls eine Referenz auf einen Funktionsbaustein (angepasst im Kundennamensraum) aufweisen.

Was bedeutet das in der Prüfung?

Fazit

Ziel der Analyse ist die Feststellung der kritischen Vergabe (mindestens) lesender Rechte auf Gehaltsbestandteile der Beschäftigten. Dabei sind sowohl die Bereiche / Zuständigkeitsgruppen als auch die Personen zu identifizieren, die einen solchen Zugriff aufweisen, um hieraus Anpassungsbedarf des Rollenmodells abzuleiten.

Darüber hinaus können auch die verschiedenen, ergänzenden Berechtigungsprüfungen identifiziert werden, die bei unterschiedlichen Funktionsprofilen gem. Tabelle T77UA und T77PR greifen, denn beliebige Funktionswahrnehmungen im Bereich der Sachbearbeitung der Personaldaten (innerhalb des Personalbereiches wie auch in weiteren Fachbereichen) können über den Aufruf eines Funktionsbausteins mit ergänzenden und beliebig umfassenden Berechtigungsprüfungen oder anderen Code-Abläufen versehen werden. Weitere Profile außerhalb des Personalbereiches sind also durchaus bedeutsam. (*FuBas können natürlich in anderen Unternehmen in Namen und Funktion differieren, die Funktionsweise ist jedoch analog anzutreffen.)*

=> SE37 nutzen und Funktionsbausteine anschauen oder bereitstellen lassen, um sie zu analysieren. Auf welche Felder in den PA-Tabellen wird referenziert?

Was bedeutet das in der Prüfung?

Dies ist sinnvoll, da hier die Funktionsübernahme-abweichende Ablaufsteuerung (PROFL) in der Personalsachbearbeitung erkannt werden kann, um die DSGVO-Konformität der Berechtigungssteuerung prüfen zu können.

- Wie viele und welche Funktionsbausteine nutzen wir im Unternehmen für eine solche Steuerung?
- Welche Profile sind mit Kundennamensraum-FuBa für welchen Zweck erweitert worden?
- Was steht in den FuBas als ergänzende Prüfung / Code-Abläufe und
- mit welchen Referenzfeldern sind sie verbunden?

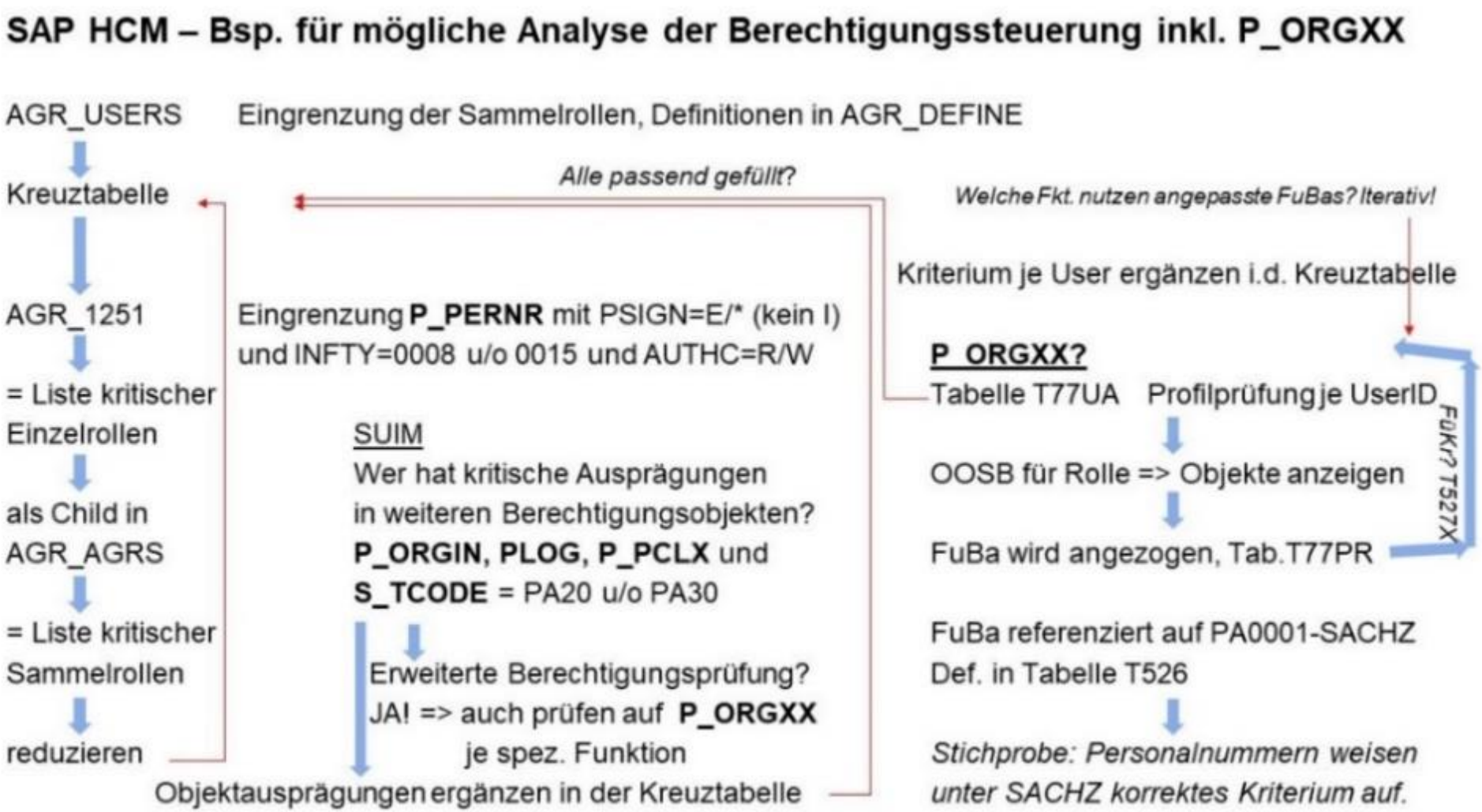
Das finale Ergebnis muss aus dem Personalbereich bestätigt werden, damit das Risiko final akzeptiert wird und die Anpassung dokumentiert gewünscht ist.

- Zusätzlich sollten auch weitere Infotypen-Zugriffe auf Rollenebene und die Leitungsebene (Vorstände / Geschäftsführung und leitende Angestellte) als Prüfungsfokus im Laufe der Zeit betrachtet werden.
- **S_TABU_DIS** benötigt zusätzlich einen Ausschluss mindestens aller PA-, SA- und SS-Tabellen (PA=Personal- [Zugriff nicht einmal lesend] & SA-/SS=Berechtigungstabellen [wenn, dann ausdrücklich nur lesend]), auch **S_TABU_NAM** sollte auf keine solcher Tabellen explizit berechtigen. Vereinzelt kommen allerdings in der Moduladministration sehr wohl aufgabenbezogen Zugriffe auf Gruppe PA vor.
- Und schließlich sollten auch Zugriffe über **S_RFC** (SE37) auf die Funktionsgruppen 7004 und BPAY im Produktionssystem unterbunden werden, da hiermit das Recht verbunden ist, unter Angabe einer beliebigen Personalnummer, z.B. mit den Bausteinen BAPI_GET_PAYSLIP, *_HTML und *_PDF, einen Abrechnungsbeleg darzustellen. Dies sollte auch die Administration nicht können! Admin-Rechte sind hier schadenfrei reduzierbar (FuGr teils remotefähig). Ggf. weitere Funktionsgruppen ausschließen?

Schlusswort

- Die BAG-Beschlüsse entfalten **Signalwirkung**, weil sie eindeutig einen Bezug des Einsichtsrechts in solche Daten zur konkreten Aufgabenwahrnehmung und dem zweckgebundenen Recht schaffen !
- Das organisatorische Gestaltungsrecht des Unternehmens bleibt unberührt. Während jedoch in anderen IT-Systemen die Rollendefinition und -wahrnehmung auch am Administrationsaufwand orientiert sein dürfen, müssen m.E. im SAP HCM die Rollendefinition und -wahrnehmung an den tatsächlichen Aufgaben und dem „Need-to-Know“-Prinzip zwingend ausgerichtet sein.
- Ein stärkeres Verteilen von privilegierten Rechten auf Gruppendefinitionen, in denen **nur zum Teil** diese Rechte benötigt werden, damit u.a. auch das Mengengerüst der Objekte im IT-System und der damit einhergehende Administrationsaufwand reduziert wird, ist **hier problematisch**. Diesen Mehraufwand muss das Unternehmen an der Stelle m.E. akzeptieren.
- Auch die Aufgabe der System- und speziell der Moduladministration mit kaum trennbaren, tiefgehenden Systemrechten ist kein genereller Sicht-Ermächtigungstatbestand. Allerdings gibt es technische Restriktionen, die vereinzelte, auch regelmäßige Tabellenzugriffe der Moduladministration auf Tabellen der PA-Gruppe notwendig machen und rechtfertigen.
- Eine Gleichschaltung der Rechte zwischen Produktion und darunterliegenden Systemen wie z.B. Test / Integration ist ebenfalls notwendig. (Datenbestände im Entwicklungssystem möglichst toolgestützt anonymisieren)

Was bedeutet das in der Prüfung?



Ich hoffe, es hat Euch gefallen und es bringt Euch weiter.

enercity AG
Konzernrevision (KR)
Christoph Wildensee

NAME	TYPE	OBJECT	FIELD	LOW	HIGH
POC_QUERY_PROCESS_REGISTRY	RF	S_RFC	ACTVT	16	
POC_QUERY_PROCESS_REGISTRY	RF	S_RFC	RFC_NAME	POC_QUERY_PROCESS_REGISTRY	
POC_QUERY_PROCESS_REGISTRY	RF	S_RFC	RFC_TYPE	FUNC	
POC_UPDATE_PROCESS_REGISTRY	RF	S_RFC	ACTVT	16	
POC_UPDATE_PROCESS_REGISTRY	RF	S_RFC	RFC_NAME	POC_UPDATE_PROCESS_REGISTRY	
POC_UPDATE_PROCESS_REGISTRY	RF	S_RFC	RFC_TYPE	FUNC	
PZ04_OLD	TR	S_RFC	ACTVT	16	
PZ04_OLD	TR	S_RFC	RFC_NAME	SLST	
PZ04_OLD	TR	S_RFC	RFC_NAME	SURL	
PZ04_OLD	TR	S_RFC	RFC_TYPE	FUGR	
PZ09	TR	S_RFC	ACTVT	16	
PZ09	TR	S_RFC	RFC_NAME	HRAC	
PZ09	TR	S_RFC	RFC_NAME	HRB2	
PZ09	TR	S_RFC	RFC_NAME	HRGL	
PZ09	TR	S_RFC	RFC_NAME	HRP3	
PZ09	TR	S_RFC	RFC_NAME	HRTM	
PZ09	TR	S_RFC	RFC_NAME	PREPTT	
PZ09	TR	S_RFC	RFC_NAME	TIQU	
PZ09	TR	S_RFC	RFC_TYPE	FUGR	
PZ11_OLD	TR	S_RFC	ACTVT	16	
PZ11_OLD	TR	S_RFC	RFC_NAME	7004	
PZ11_OLD	TR	S_RFC	RFC_NAME	HRO1	
PZ11_OLD	TR	S_RFC	RFC_NAME	SLST	
PZ11_OLD	TR	S_RFC	RFC_NAME	SURL	
PZ11_OLD	TR	S_RFC	RFC_TYPE	FUGR	
PZ17_OLD	TR	S_RFC	ACTVT	16	
PZ17_OLD	TR	S_RFC	RFC_NAME	SLST	
PZ17_OLD	TR	S_RFC	RFC_NAME	SURL	
PZ17_OLD	TR	S_RFC	RFC_TYPE	FUGR	
PZ35_MA	TR	S_RFC	ACTVT	16	
PZ35_MA	TR	S_RFC	RFC_NAME	HR_ESS_WHO	
PZ35_MA	TR	S_RFC	RFC_TYPE	FUGR	
PZFOTO	TR	S_RFC	ACTVT	16	
PZFOTO	TR	S_RFC	RFC_NAME	HR_ESS_MINIAPP	
PZFOTO	TR	S_RFC	RFC_TYPE	FUGR	
PZLE	TR	S_RFC	ACTVT	16	
PZLE	TR	S_RFC	RFC_NAME	EH08	
PZLE	TR	S_RFC	RFC_NAME	RFC1	
PZLE	TR	S_RFC	RFC_NAME	SDIF	
PZLE	TR	S_RFC	RFC_NAME	SU_USER	
PZLE	TR	S_RFC	RFC_NAME	SWOR	
PZLE	TR	S_RFC	RFC_NAME	SYSU	
PZLE	TR	S_RFC	RFC_TYPE	FUGR	
PZM3_START_MA	TR	S_RFC	ACTVT	16	
PZM3_START_MA	TR	S_RFC	RFC_NAME	EHSS	
PZM3_START_MA	TR	S_RFC	RFC_TYPE	FUGR	

Anhang
S_RFC bei Admins

Data Browser: Tabelle USOBT: Selektionsbild

Anzahl Einträge

NAME		bis
TYPE		bis
OBJECT	S_RFC	bis
FIELD		bis
LOW	7004	bis

Spannend:

Tabelle USOBT ergibt für Transaktionen, die auf S_RFC zugreifen müssen und eine Gruppeneingrenzung auf 7004 benötigen, nur einen Treffer: PZ11_OLD.
Ist dies eine Transaktion, die ein Personaler, Moduladministrator oder Systemadministrator benötigt? Personalbereich hat Alternativen.
FuGr BPAY = keine Transaktionen, kann also auch entfernt werden.
Was ist z.B. mit der Gruppe HR_INFOTYPE8_PAYROLL und dem Baustein HR_PAYROLL_TEST_PAYSLIP_SHOW ?

Anhang
S_RFC bei Admins

Data Browser: Tabelle USOBT 10 Treffer

Prüftabelle...

Tabelle: USOBT
Angezeigte Felder: 9 von 9 Feststehende Führungsspalten: 5 Listbreite 0250

NAME	TYPE	OBJECT	FIELD	LOW	HIGH
PC00_M01_RPUZVMD2	TR	S_RFC	RFC_NAME	HRPBSDEZV_DCARRIER_RFC	
PECM_ADJ_SAL_STRU	TR	S_RFC	RFC_NAME	HRECM00JPRSALARYADJUSTMENT	
PZ09	TR	S_RFC	RFC_NAME	HRAC	
PZ09	TR	S_RFC	RFC_NAME	HRB2	
PZ09	TR	S_RFC	RFC_NAME	HRGL	
PZ09	TR	S_RFC	RFC_NAME	HRP3	
PZ09	TR	S_RFC	RFC_NAME	HRTM	
PZ11_OLD	TR	S_RFC	RFC_NAME	HRO1	
PZ35_MA	TR	S_RFC	RFC_NAME	HR_ESS_WHO	
PZFOTO	TR	S_RFC	RFC_NAME	HR_ESS_MINIAPP	

Aus Tabelle USOBT nur diese P- und S-Transaktionen, die auf S_RFC zugreifen müssen und eine Gruppeneingrenzung auf eine Gruppe aus HR* benötigen. Bei S-Transaktionen keine einzige, die auch auf S_RFC mit einer HR*-Eingrenzung zugreifen muss. Auch keine mit HR_INFOTYPE8_PAYROLL und dem Baustein HR_PAYROLL_TEST_PAYSLIP_SHOW (→ Abrechnungssimulationsbaustein).

Somit ratsam: Herausnahme von 7004, BPAY und HR_I* !! und Prüfung, ob es noch weitere FuBa gibt, wo die Gruppe aus den Berechtigungen herausgenommen werden sollte.