Vereinbarung nach § 94 HmbPersVG
über die Vergabe von Zugriffsrechten
bei der Einführung und Nutzung des SAP R/3 – Verfahrens zur integrierten Ressourcensteuerung

zwischen

der Freien und Hansestadt Hamburg
vertreten durch den Senat
Personalamt

einerseits

und

dem DBB Hamburg
- Beamtenbund und Tarifunion –

dem Deutschen Gewerkschaftsbund
- **Landesbezirk Nord –**
-
als Spitzenorganisationen der Gewerkschaften

andererseits

wird Folgendes vereinbart:

1. Ziele dieser Vereinbarung

In der Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung eines Verfahrens zur integrierten Ressourcensteuerung haben sich die Partner dieser Vereinbarung darauf verständigt, die erforderlichen Konkretisierungen des Einführungskonzepts im Koordinierungsausschuss zu beraten und ggf. gesondert zu vereinbaren.

Ein wesentliches Element zum Schutz der Mitarbeiterinnen und Mitarbeiter bzw. ihrer Daten vor unzulässigen Leistungs- und Verhaltenskontrollen und unberechtigter Einsichtnahme sind verlässliche Grundsätze und ein geregeltes Verfahren zur Vergabe der Zugriffsrechte auf die unter SAP R/3 gespeicherten Daten. Beispiele für personenbezogene Daten sind Auszahlungen an Mitarbeiterinnen und Mitarbeiter im Rahmen der Mittelbewirtschaftung und die Daten in den personenbezogen auswertbaren Systemprotokolldateien.

Das "SAP R/3 Berechtigungskonzept[1]" dient sowohl den Sicherheitsanforderungen eines Verfahrens zur Unterstützung des Haushalts-, Kassen- und Rechnungswesens als auch dem Schutz der vorstehenden personenbezogen Daten. Es soll eine transparente und nachvollziehbare Vergabe der Zugriffsrechte im R/3-System sicherstellen und damit Vertrauen bei den Mitarbeiterinnen und Mitarbeitern in den angemessenen Umgang mit ihren Daten schaffen.

Die 94er-Partner sind sich einig, dass das Berechtigungskonzept einer laufenden Weiterentwicklung unterliegt. Diese Vereinbarung formuliert daher Anforderungen an die Berechtigungsvergabe bzw. das Berechtigungskonzept, die dabei auch in Zukunft zu erfüllen sind[2] und deren organisatorische und technische Umsetzung der jeweils gültigen Fassung des Berechtigungskonzeptes zu entnehmen ist.

Mit dem Abschluss dieser Vereinbarung soll der Bedeutung der zu Grunde liegenden Ziele Rechnung getragen und für die Einführungsprozesse in den Fachbehörden eine verbindliche Grundlage zur Verfügung gestellt werden.

Die Finanzbehörde wird für die laufende Aktualisierung des Berechtigungskonzeptes Sorge tragen.

2. Anforderungen an das Berechtigungskonzept für SAP R/3

Bei der Erstellung eines Berechtigungskonzepts sind die Anforderungen des Hamburgischen Datenschutzgesetzes sowie die Mitbestimmungsrechte der Personalräte zu berücksichtigen.

2.1 Nachvollziehbarkeit

Die Grundsätze und Verfahren der Berechtigungsvergabe werden in einer Weise beschrieben, die in Kernaussagen ohne SAP-Fachtermini auskommt und auch für Personen verständlich ist, die als Mitarbeiterinnen und Mitarbeiter der Behörden bzw. als Personalratsmitglieder mit der Sache befasst sind, aber nicht über Detailkenntnisse des SAP-Systems verfügen

Es gilt ein behördenübergreifend einheitliches Verfahren der Berechtigungsvergabe, bei dem mindestens ein 4-Augen-Prinzip technisch sichergestellt ist. Niemand darf in der Lage

[1] Grundlage ist das Berechtigungskonzept Version 2.1 vom 02.05.2002

[2] Sofern nicht ausdrücklich anders vereinbart, gelten diese Anforderungen an die Berechtigungsvergabe für das SAP R/3 "Produktionssystem".

sein, einen neuen SAP-User sowohl allein einzurichten, als auch nachfolgend zu aktivieren und zu nutzen. Mindestens eine dieser drei Aktivitäten ist von einer zweiten Person durchzuführen.

Für die Benutzerverwaltung wird in der FHH das elektronische Benutzerverwaltungsverfahren genutzt.

Die Zugriffsrechte sollen in der Regel so angelegt werden, dass sie für mehrere Systembenutzerinnen und -benutzer gelten. Benutzerinnen und Benutzer mit gleichen fachlichen Aufgaben im gleichen Bereich erhalten erkennbar die gleichen Zugriffsrechte (in SAP: "Aktivitätsgruppe" bzw. "Rolle"). Dies gilt auch für Benutzerinnen und Benutzer mit Aufgaben der zentralen oder dezentralen Systemverwaltung. Der Grundsatz der Beschränkung der Zugriffsrechte auf das für die Aufgabe notwendige ist auch hier anzuwenden.

Für die technische Bezeichnung der Zugriffsrechte werden Namenskonventionen verwendet, die einen eindeutigen Zusammenhang zur Fachaufgabe erkennbar machen.

Es wird dafür Sorge getragen, dass Änderungen im Berechtigungssystem dauerhaft protokolliert werden.

2.2 Vollständigkeit und Einheitlichkeit

Das Berechtigungskonzept zum SAP R/3 – System soll Zugriffsmöglichkeiten und -rechte auf die im SAP R/3-System gespeicherten Daten, die auf der Ebene des Betriebssystems, des Netzes oder der Datenbank bestehen oder die sich aus Schnittstellen ergeben, zumindest summarisch benennen. Insbesondere werden die Rollen benannt, die die Möglichkeit beinhalten, Daten zur Weiterverarbeitung in andere Anwendungen zu übertragen. Dies umfasst die sogenannte Download-Funktion und den Datenexport über Schnittstellen.
Die Möglichkeiten des Zugriffs auf die SAP R/3 Datenbank SQL 2000 werden in der Anlage 1 zu dieser Vereinbarung beschrieben.

Die Zugriffsrechte auf die im SAP R/3 – System zur integrierten Ressourcensteuerung gespeicherten Daten und die Verfahren zu ihrer Vergabe werden auf allen organisatorischen Ebenen beschrieben. Sofern in den Fachbehörden Konkretisierungen der allgemein gültigen Regeln oder Abweichungen davon erfolgen, werden sie in eigenen, behördenspezifischen Berechtigungskonzepten dargestellt. Sofern in einer Behörde zwei oder mehrere Buchungskreise eingerichtet werden, bedarf es buchungskreisspezifischer Berechtigungskonzepte. Die hier vereinbarten Grundsätze gelten auch für diese Berechtigungskonzepte.
Die behördenspezifischen Berechtigungskonzepte regeln die Zugriffsmöglichkeiten auf das Entwicklungs-, das Qualitätssicherungs- und das Produktivsystem.

Mindestinhalte der behördenspezifischen Berechtigungskonzepte sind

- die Auflistung der SAP R/3-Module, die in der Behörde eingesetzt werden,
- die Geschäftsprozesse/-vorfälle, die unter Nutzung der SAP R/3-Module in der Behörde durchgeführt werden,
- die Gruppierung der SAP R/3-Benutzer der Behörde nach Aufgaben (Rollen),
- die Darstellung kritischer Transaktionen im SAP R/3-System und getroffene Schutzmaßnahmen,
- die Organisationsstammdaten für die elektronische Benutzerverwaltung.

2.3 Datenschutz

Das Berechtigungskonzept soll zur Umsetzung von Anforderungen aus dem Hamburgischen Datenschutzgesetz beitragen.

Die Verhandlungspartner haben eine Liste kritischer Buchungsvorgänge im Rahmen der integrierten Ressourcensteuerung erstellt (siehe Anlage 2). Sofern diese Buchungen zwingend in SAP erfolgen müssen, ist für die Abwicklung dieser Buchungen für jede Behörde ein eigener Geschäftsbereich in SAP einzurichten. Personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter werden nur innerhalb dieses Geschäftsbereiches auf eigens dafür eingerichtete Finanzstellen und Kostenstellen kontiert. Dabei ist die Zahl der Zugriffsberechtigten deutlich einzuschränken.

Das Zugriffsrecht auf diesen Geschäftsbereich soll der Personalabteilung vorbehalten sein.

Ist dies nicht möglich, sind die Zugriffsrechte im Rahmen einer Dienstvereinbarung zu regeln; die betreffenden Anwenderinnen und Anwender sind den für die Mitarbeiterinnen und Mitarbeiter von Personalabteilungen geltenden Regeln des Datenschutzes zu unterwerfen.

Die Kassenabteilung wird sich bei der Aufklärung von Zahlungseingängen auf Verwahrkonto, die erkennbar einen Bezug zu Beschäftigten der Freien und Hansestadt Hamburg haben, nur derjenigen Mitarbeiterinnen und Mitarbeiter der Behörden und Ämter bedienen, die auch Zugriff auf den Geschäftsbereich Personal besitzen.

Bei Mitarbeiterdaten, die als kritisch anzusehen sind, wird eine "Download"-Berechtigung in den Standard-Rollen nicht vorgesehen (zum gegenwärtigen Zeitpunkt betrifft dies ausschließlich Rollen mit Zugriff auf Daten aus der Zeiterfassung in CATS).

2.4 Kontrolle

Die Finanzbehörde trägt dafür Sorge, dass die Einhaltung des Berechtigungskonzeptes regelmäßig überprüft wird.

Insbesondere ist im Produktivsystem eine regelmäßige Kontrolle der Benutzerberechtigungen durchzuführen und sicherzustellen, dass die im Berechtigungsrahmenkonzept dokumentierten Vorgaben zur Zuordnung von Benutzern zu Rollen eingehalten werden und Benutzerstämme gelöscht/gesperrt/geändert werden, wenn Mitarbeiterinnen oder Mitarbeiter die FHH verlassen oder in andere Bereiche mit anderen Aufgaben versetzt werden.

Von der Finanzbehörde wird ein Berechtigungsprofil zur temporären Vergabe entwickelt und bereitgehalten, das es ermöglicht, die Einhaltung der Bestimmungen dieser Vereinbarung bei Bedarf am SAP-System zu überprüfen. Dieses Berechtigungsprofil steht den Behörden zur Verfügung, sofern von Personalräten eine Überprüfung gewünscht wird. Ein entsprechender Hinweis wird unter dem Punkt "Sondernutzer" in das Berechtigungskonzept aufgenommen.

In Abstimmung mit den Spitzenorganisationen wird ein Seminar für Personalräte entwickelt und regelmäßig mindestens alle drei Jahre angeboten, das Grundzüge des Berechtigungssystems und die Grundsätze der Berechtigungsvergabe nach dem geltenden Berechtigungskonzept vermitteln soll. Dazu gehört ein Überblick über die im SAP-System vorhandenen Möglichkeiten zur Überprüfung der Berechtigungsvergabe.

3. Einzelne Anforderungen

Es soll technisch so weit wie möglich ausgeschlossen werden, dass eine einzelne Person vollständige Kontrolle über das SAP R/3-System erlangt.

Berechtigungen zur Programmierung, zur Veränderung von Systemeinstellungen (SAP: "Customizing") oder andere weitreichende Rechte zu Änderungen am SAP R/3-System sollen in der Regel im "Produktionssystem" nicht vergeben werden. Zeitweilig notwendige Ausnahmen für das Customer Competence Center oder die fachliche Leitstelle sind so zu gestalten, dass die Nutzung erkennbar und nachvollziehbar bleibt.

4. Geltungsbereich

Diese Vereinbarung gilt für alle Beschäftigten, die das SAP R/3 Verfahren zur integrierten Ressourcensteuerung nutzen.

5. Schlussbestimmungen

Diese Vereinbarung tritt mit sofortiger Wirkung in Kraft. Sie kann mit einer Frist von sechs Monaten zum Ende eines Jahres gekündigt werden.

Bei Kündigung wirkt diese Vereinbarung bis zum Abschluss einer neuen Vereinbarung nach.

Hamburg, den ……..

Senat der Freien und Hansestadt Hamburg
- Personalamt -

……

DBB Hamburg
- Beamtenbund und Tarifunion -

……..

Deutscher Gewerkschaftsbund
- Landesbezirk Nord -

……

Möglichkeiten des Zugriffes auf die SAP R/3 Datenbank Microsoft – SQL Server

Neben den Zugriffen, die durch die Anwendung SAP dargestellt und geregelt sind, gibt es noch folgende Möglichkeiten auf Systemebene:

Das „Relationale Datenbank Management System“ Microsoft – SQL Server (in der Version SQL 2000 oder höher) ist das Trägersystem für die SAP relevanten Objekte, Tabellen, Ansichten und Daten. Dieses transaktionsgesteuerte Datenbanksystem schreibt bei der Verarbeitung die ausgeführten, zur Veränderung führenden Transaktionen in so genannte Transaktions-Logs. Diese Logs sind Bestandteile des Gesamtsystems und ermöglichen bei Fehlersituationen ein Rollback der Transaktionen. Auf diese Weise können Recovery-Maßnahmen zeitgenau und transaktionsspezifisch ausgeführt werden.

Diese Dateien können nur von einem autorisierten Systemadministrator dem System zugeführt werden; Zugriffe auf die Datenbank sind ohne entsprechende Maßnahmen eines Systemadministrators nicht möglich. Beim SQL-Server gibt es eine explizite Benutzerverwaltung, die die Zugriffsmöglichkeiten auf dieses System regelt – ohne diese Benutzerverwaltung kann eine Anwendung den SQL-Server nicht nutzen.

Sie sieht vor, dass

- SAP die einzig zugelassene Anwendung mit Zugriff auf die ihr zu Grunde liegende Datenbank ist,
- Datenbankexporte, Datenbanksicherung und Datenrücksicherung als die weitreichendsten Rechte außerhalb von SAP nur Systemadministratoren gestattet ist,
- es Anwenderinnen und Anwendern mit weitgehenden Rechten in SAP unmöglich gemacht wird, Administrationsrechte für die Datenbank zu erlangen.

Bei einer Tabellenanzahl von ca. 24.000 Tabellen ist darüber hinaus ein Zugriff auf einzelne oder mehrere Tabellen ohne Kenntnis der entsprechenden Geschäftslogik völlig sinnlos. Zusätzlich ist auch anzumerken, dass der Inhalt vieler Tabellen (die tatsächliche Anzahl ist nicht quantifizierbar) keinen Klarschrift-Inhalt hat, sondern vielfach hexadezimal und verschlüsselt ist.