

# SAP Spezial 1

***Gesundheitswesen***

***Datenschutz***

***Dr. H. Haaz***

- ➔ Dr. Heiko Haaz
- ➔ Industriekaufmann; Studium der Wirtschaftswissenschaften, Abschluß Diplom-Kaufmann
- ➔ Datenschutzberatung in verschiedenen Branchen
- ➔ Datenschutzbeauftragter in verschiedenen Unternehmen/Branchen
- ➔ Dissertation:  
Der Datenschutzbeauftragte: Aufgaben und Anforderungen des Tätigkeitsfeldes eines Datenschutzbeauftragten; Organisatorische Merkmale, Rechtliche Aspekte, Konkrete Lösungsansätze
- ➔ Partner der UIMC

## Aktivitätenfelder

Individuelle Beratungen und Konzeptionen	Standardisierte Beratungen und Konzeptionen	Sondergebiete	Betriebliche und außerbetriebliche Fort- und Weiterbildung
Unternehmensführung	<b>UMC</b> - Unternehmens- und Management-Checkup	IV-Sicherheit	Unternehmensorganisation
Controlling	<b>Si-SSA</b> Sicherheits-Schwachstellenanalyse für Informationssysteme - Allgemeine Si-SSA - Sicherheits-Checkup für - KIS (Krankenhausinformationssysteme) - PRAIS (Praxisinformationssysteme)	Datenschutzberatung gem. BDSG	Unternehmensplanung und -budgetierung
Aufbau- und Ablauforganisation		IV-Revision (Auditing)	IV-Systemplanung
Planung und Budgetierung	<b>DC</b> - Datenschutz-Checkup gem. BDSG und IuKDG	Datenschutz und -sicherheit im Gesundheitssektor	Controlling
Informationssystemmanagement		externe Datenschutzbeauftragung	IV-Controlling
Marketing		Erstellen und Überprüfen von Pflichtenheften	Sicherheitskonzeptionen
			IV-Arbeitsplatzsicherheit

## Grundsatz im Datenschutz

**Die Verarbeitung von personenbezogenen Daten  
ist verboten**

es sei denn, es wird erlaubt!

## Blick in das Gesetz - Praxis

- Die Zulässigkeit der Datenverarbeitung muss in jeder Phase gegeben sein. Insbesondere muss die Erhebung, Speicherung, Veränderung, Nutzung oder Übermittlung zulässig sein.
- Die Verarbeitung darf nur zweckgebunden erfolgen.
- Das Gebot der Datensparsamkeit und Datenvermeidung ist zu beachten.
- Die Anforderungen des § 9 BDSG (und Anlage) sind umzusetzen.
- Die Verpflichtung der Beschäftigten auf das Datengeheimnis ist zu beachten.
- Gewährleistung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung bzw. Löschung.

## Blick in das Gesetz - Praxis

- Es sollte eine prüfbare Gestaltung des Verfahrens existieren.
- Bei besonderen Daten ist eine Vorabkontrolle durchzuführen.
- Es ist eine Verfahrensübersicht (§ 4 e) zu erstellen.
- Aufgabe des Datenschutzbeauftragten ist es, auf die Einhaltung der Datenschutzgesetze hinzuwirken.

1. Teilprojekt Abrechnung & Personaladministration
2. Teilprojekt Personalbeschaffung
3. **Teilprojekt Schulungen**
  - Einbinden des Themas Datenschutz in die Schulungen
  - Schulungen für die Betriebsräte
  - Benutzerschulungen
  - Teilnahme des DSB an Schulungen (als Teilnehmer)
4. Teilprojekt Organisationsmanagement
5. Teilprojekt Zeitwirtschaft
6. Teilprojekt Schnittstelle
7. Teilprojekt Prozesse
8. **Teilprojekt Dienstvereinbarung & Datenschutz**
9. Teilprojekt Technik

## TP Dienstvereinbarung & Datenschutz

- Dienstvereinbarungen
- Infotypen incl. Herkunft
- Berechtigungen
- Sicherheitskonzept
- Dokumentationen

# Dienstvereinbarung

Warum ist dies für den DSB wichtig?

GBV Nr. XX: Gesamtbetriebsvereinbarung zu SAP

- § 1 Zielsetzung und Nutzungsumfang
- § 2 Schutz der Mitarbeiterdaten
- § 3 Schnittstellen
- § 4 Leistungs- und Verhaltenskontrollen
- § 5 Zeiterfassung
- § 6 Qualifizierung und Weiterbildung
- § 7 Rechte der Mitarbeiter
- § 8 Rechte des Betriebsrates
- § 9 Schlussbestimmungen

*Anlagen:*

*Anlage 1:* Liste der Info- und Infosubtypen

*Anlage 2:* Liste der Auswertungen

*Anlage 3:* Benutzerrollen

*Anlage 4:* Einstellungen eines Security Audits

# Infotypen

Dies sind die Datenfelder im SAP

Bsp: Infotyp 0002 „ Daten zur Person“

## Name

- Anrede
- Nachname
- Titel
- Vorname
- Initialen
- Vorsatzwort
- Zusatzwort
- Aufbereitung
- Sonderform

## Geburtsdaten

- Geburtsname
- Vorsatzwort
- Zusatzwort
- Geburtsdatum
- Geburtsort
- Kommunikationssprache
- Geburtsland
- Nationalität
- Nationalität 2
- Nationalität 3

## Familienstand/Konfession

- *Familienstand*
- *Familienstand seit*
- *Anzahl Kinder*

## Infotypen

- Abschließende Vereinbarung über Einsatz der Infotypen
- Prüfung auf Zulässigkeit
- Beachtung von Notwendigkeiten

# Berechtigungen

## SAP Berechtigungshandbuch

### Inhaltsverzeichnis

- 1 Einleitung
  - 1.1 Zuständigkeiten
  - 1.2 Wichtige Begriffe
  - 1.3 Konzeptionelle Probleme bei SAP R/3
- 2 Verteilung von Mitarbeiterdaten und Probandendaten auf SAP-Systeme
  - 3.1 Technischer Aufbau / Pflege des SAP-Berechtigungskonzepts
  - 3.2 Ersterstellung der Unternehmensfunktionen in Form von Berechtigungsrollen
- 4 **Allgemeine Regelungen (s. Datenschutzhandbuch)**
  - 4.1 **Allgemeine Zugriffsregelungen**
  - 4.2 **Rechtebeantragung**
  - 4.3 **Regeln für Passwörter (Kapitel 4.3.2 des Datenschutzhandbuches)**
- 5 Organisatorischer Aufbau der Funktionen

# Berechtigungen

## SAP Berechtigungshandbuch

### Inhaltsverzeichnis

- 6 Regelung der Zuordnung von Funktionen / Rollen
  - 6.1 Namenskonventionen bei Rollen**
  - 6.2 Profilname
  - 6.3 Organisatorischer Aufbau der Berechtigungsrollen
- 7 HR Rollen
- 8 EH&S
- 9 Berechtigungskonzept im Bereich QM
  - 9.1 Profil Q:QM\_MELER
  - 9.2 Profil Q:QM\_MELMB
- 10 Berechtigungen CO

# Berechtigungen

## SAP Berechtigungshandbuch

### Inhaltsverzeichnis

- 11 Namensvergabe von User-Stammsätzen
  - 11.1 Kritische Berechtigungsobjekte**
  - 11.3 Kritische Kombination von Berechtigungsobjekten und Transaktionen
  - 11.4 Kritische Transaktionen
  - 11.5 Gesperrte Transaktionen
  - 11.6 RFC / CPIC – Remote Zugriff
- 12 Berechtigungsprofile SAP\_ALL, SAP\_NEW und P\_BAS\_ALL
  - 12.1 Behandlung der Sonderbenutzer (SAP\*, DDIC, CPIC, Early Watch, ADMIN, SAPX25)**
  - 12.2 Schutzmaßnahmen für SAP – Standarduser und Sonderbenutzer
- 13 Verfahren der Benutzereinrichtung
- 14 Die Protokollierung der Sonderbenutzer mit Security Audit Log
- 15 Weiterführende Dokumente

# Berechtigungen

## 4.1 Allgemeine Zugriffsregelungen

- Die Veränderung von Zugriffsrechten ist zu dokumentieren.
- Das Ausscheiden von Mitarbeitern ist sofort der EDV-Abteilung mitzuteilen, damit diese umgehend alle Zugriffsrechte löschen kann.
- Eine längere Abwesenheit (mehr als 6 Wochen) von Mitarbeitern ist der EDV-Abteilung von der zuständigen Personalabteilung mitzuteilen. Dieser sperrt dann die Zugriffsrechte.
- Bei befristeten Arbeitsverhältnissen (Zeitarbeitskräfte, Praktikanten etc.) sind die Zugriffsrechte nur mit zeitlicher Begrenzung zu beantragen.
- Sollten Mitarbeiter Zugriffe außerhalb der regulären Arbeitszeit benötigen, so ist dies bei der EDV-Abteilung zu beantragen und zu begründen.

Um unzulässige Zugriffe abzuwehren, gilt:

- Kein Benutzer darf sich gleichzeitig an mehreren Arbeitsplätzen anmelden können.
- Jeder Benutzer hat sich bei längerem Verlassen des Arbeitsplatzes abzumelden.

# Berechtigungen

## 4.2 Rechtebeantragung

- Zugriffsrechte sind von dem jeweiligen Organisationsleiter bei der DV-Abteilung schriftlich zu beantragen. Eine mündliche Beantragung ist nicht zulässig.
- Zugriffsrechte sind auf die für die Aufgabenerfüllung notwendigen Rechte zu beschränken. Sie sind restriktiv zu vergeben. Es ist festzulegen, wer welche Daten lesen, löschen, hinzufügen oder verändern darf.
- Schreibrechte sind nur dann zu erteilen, wenn reine Leserechte nicht ausreichen.
- Die Festlegung von Zugriffsrechten ist zu dokumentieren. Darüber hinaus ist den Benutzern eine schriftliche Aufstellung ihrer Zugriffsrechte zu übergeben und sie müssen durch ihre Unterschrift erklären, dass sie die Zugriffsbedingungen verstehen.

# Berechtigungen

## 6.1 Namenskonventionen bei Rollen

Die für eine Unternehmensfunktion erstellte Berechtigungsrolle unterliegt einer Namenskonvention, die von dem Berechtigungsverwaltungsprogramm BKZ vorgegeben wird.

Bis Doppelpunkt Modul z. B.

FI	Finanzen
CO	Controlling
CS	Customer Service
EH&S	EH&S

usw. bis Doppelpunkt

Ab Doppelpunkt

Stelle 1 - 7

Textbeschreibung der Rolle

Stelle 8

1 = Anzeige, 2 = Pflege

Stelle 9 - 15

lfd. Nummer (Unterscheidungsmerkmal für die Tochterrollen)

Bsp: QM:MELDUNG1000007

# Berechtigungen

## 11.1 Kritische Berechtigungsobjekte

Folgende Berechtigungsobjekte werden im Produktivsystem keinem Anwender zugeordnet.

<b>Berechtigungsobjekt</b>	<b>Beschreibung</b>
S_ADMI_FCD	Systemberechtigungen
S_ARCHIVE	Archivierung
S_DATASET	Berechtigung zum Dateizugriff
S_ENQUEUE	Enqueue: Anzeigen und Löschen von Sperreinträgen
S_NUMBER	Nummernkreispflege
S_TABU_DIS	Tabellenpflege (über Standardwerkzeuge, z. B. SM30)
.....	

## Berechtigungen

### **12.1 Behandlung der Sonderbenutzer (SAP\*, DDIC, CPIC, Early Watch, ADMIN, SAPX25)**

Neben den im Berechtigungskonzept spezifizierten Berechtigungen werden für bestimmte administrative Aufgaben zeitweise zusätzlich die Sonderbenutzer SAP\*, DDIC, NotfallUser ADMIN und SAP-Fernwartunguser SAPX25 mit umfangreichen Systemrechten benötigt. Beispiele für solche Aufgaben sind:

- die erweiterte Nutzung des Korrektur- und Transportwesens bei Aktivierung von Programmen und speziellen Elementen des Data Dictionary
- die Planung und Durchführung von Releasewechsel
- Schutz eines Systems vor Anmeldung durch Sperrung bei Wartungsaktivitäten

Die Nutzung dieser Sonderbenutzer SAP\* und DDIC ist dem RZ vorbehalten. Der Notfalluser wird modulabhängig vergeben. Der SAP-Fernwartunguser wird ausschließlich von der SAP benutzt.)

.....

# Sicherheitskonzept

## Gliederung

- 1 Einleitung
- 2 Strukturorganisatorische Richtlinien
- 3 Übergreifende Richtlinien
- 4 Verwaltung des IT-Systems
- 5 Berechtigungsorientierte Sicherheitsmaßnahmen
- 6 Arbeitsplatzorientierte Sicherheitsmaßnahmen
- 7 Kommunikationsspezifische Richtlinie
- 8 Richtlinien für Notfall-, Katastrophen- und Wiederanlaufplanung
- 9 Allgemeine datenschutzrelevante Richtlinien für Mitarbeiter
- 10 Spezielle datenschutzrelevante Richtlinien
- 11 Gesetzesspezifische Richtlinien
- 12 Vertragsspezifische Richtlinien
- 13 Prüfungsnormen und -vorgaben

## Organisation

- SAP Betriebshandbuch
- SAP Berechtigungshandbuch
- Betriebsvereinbarungen
- Sicherheitskonzept
- Notfallplanungen
- Verfahrensabläufe

**UIMC**<sup>®</sup>

**Ihre Partner**

**in Datenschutz und IT-Sicherheit!**

**UIMC**<sup>®</sup>

**DR. VOSSBEIN  
GmbH & Co KG**

UIMC Dr. Vossbein GmbH & Co. KG

Nützenberger Straße 119

42115 Wuppertal

Telefon: (0202) 265 74 - 0

Telefax: (0202) 265 74 - 19

E-Mail: [consultants@uimc.de](mailto:consultants@uimc.de)

URL: [www.UIMC.de](http://www.UIMC.de)

**Neu!**  
**UIMCollege**<sup>®</sup>

**UIMCert**<sup>®</sup>  
**GMBH**

UIMCert GmbH

Moltkestraße 19

42115 Wuppertal

Telefon: (0202) 3 09 87 39

Telefax: (0202) 3 09 87 49

E-Mail: [certification@uimcert.de](mailto:certification@uimcert.de)

URL: [www.UIMCert.de](http://www.UIMCert.de)