

DSAG Arbeitskreis Revision Arbeitsgruppe Datenschutz

Leitfaden Datenschutz für SAP BW

Release 3.1
Stand 28. November 2003

<http://www.sap.de/revis>



SAP® AG • Neurtstr. 16 • D-69190 Walldorf
Änderungen und Ergänzungen vorbehalten

Leitfaden Datenschutz für SAP BW

Einleitung	5
0 Einführung	7
1 Rechtliche Anforderungen an ein SAP Business Warehouse (BW)	10
2 SAP-Fakten und Datenschutzaspekte	15
2.1 Datenbereitstellung und Datenhaltung.....	15
2.1.1 DataSource.....	16
2.1.1.1 Persistent Staging Area	17
2.1.1.2 Metadata Repository	18
2.1.2 InfoObjects	18
2.1.4 Operational Data Store	20
2.1.5 InfoCube	20
2.1.5.1 Fortschreibung.....	21
2.1.5.2 Sternschema	21
2.1.5.3 Aggregat.....	21
2.1.6 Business Content	22
2 Einführungsmethoden	24
2.2.1 ASAP und Solution Manager	25
2.2.1.1 Projektvorbereitung.....	25
2.2.1.2 Business Blueprint.....	25
2.2.1.3 Realisierungsphase	26
2.2.1.4 Produktionsvorbereitung, bzw. Final Preparation.....	27
2.2.1.5 Go Live and Support	27
2.2.1.6 Empfehlung zur Vorgehensweise.....	28
2.2.2 Business Content	28
2.3 Übersichten	31
2.4 Auftragsdatenverarbeitung.....	36
2.5 Datenübernahme (Anonymisierung, Pseudonymisierung)	37
2.5.1 Anonymisierung oder Pseudonymisierung bei Übernahme	37
2.5.2 Anonymisierung bei Query-Erstellung.....	41
2.5.3 Datenalterung und Archivierung	41
2.6 Sichten / Auswertungen	42
2.6.1 Auswertungswerkzeuge.....	42
2.6.2 Auswertungsmöglichkeiten	44
2.6.3 Zugriffsrechte bei selbstentwickelten Auswertungen.....	45
2.6.4 Auswertungen des Business Content.....	46
2.6.4.1 Beispiele aus nicht HR-Anwendungen	48
2.6.4.2 Business Content für HR-Daten.....	49
2.7 Umsetzung der Anforderungen aus § 9 BDSG und Anlage: technisch-organisatorische Maßnahmen.....	53
2.7.1 Anforderungen.....	53
2.7.2 SAP-Fakten, Risiken und Maßnahmen	54
2.7.2.1 Identifizierung und Authentifizierung.....	54

2.7.2.2 Standardbenutzer	54
2.7.2.3 Benutzerberechtigungskonzept: Berechtigungsobjekte für BW	54
2.7.2.4 Benutzerberechtigungskonzept: Rollen für das BW	62
2.7.2.5 Benutzerberechtigungskonzept: fachliche Ausgestaltung.....	63
2.7.2.6 Besonderheiten bei der Berechtigungsprüfung	65
2.7.2.7 Benutzer- und Berechtigungsadministration	65
2.7.2.8 Änderungen am Produktivsystem	66
2.7.2.9 Systemschnittstellen	66
2.7.2.10 Auditing und Logging	67
2.7.2.11 Zusammenhang Leitfäden Datenschutz R/3 - BW	67
3 Risiken / Bewertung der Fallgruppen	69
3.1 Zusammenfassung zentraler Risiken	70
3.2 Zusammenfassung der Prüfungshandlungen	70
3.2.1 Anforderungen an die Prüfbarkeit	70
3.2.2 Prüfung spezieller Regelungen aus vorrangigen Rechtsvorschriften	72
3.2.3 Prüfung der Datenschutzmaßnahmen gemäß § 9 BDSG und Anlage	72
4 Literaturverzeichnis	75
5 Index	76
Glossar.....	77

Einleitung

Dieser Leitfaden beschreibt für Datenschutzbeauftragte der SAP-Anwender und Berater datenschutzrechtliche Anforderungen sowie technische Fakten zum SAP Business Information Warehouse (SAP BW Rel. 3.1 Content) und gibt Hinweise zu Risiken, deren Bewertung sowie entsprechenden Prüfhandlungen.

Er ergänzt den SAP Sicherheitsleitfaden sowie den *Leitfaden Datenschutz für SAP R/3* und ist wie diese nur als Empfehlung zu verstehen. Die Verantwortung für die Einhaltung der Datenschutzvorschriften verbleibt bei den Firmen und deren Datenschutzbeauftragten. Datenschutzrechtliche Grundlagen sind die EU-Richtlinie 95/46/EG und das deutsche Bundesdatenschutzgesetz BDSG 2001¹

Erstellt wurde dieser Leitfaden von Mitgliedern der Arbeitsgruppe Datenschutz im DSAG Arbeitskreis Revision/Risikomanagement, die hiermit ihre Erfahrungen zur Verfügung stellen. Die meisten der Autoren waren auch an der Erstellung des *Leitfaden Datenschutz für SAP-R/3* Release 4.6 beteiligt.

© Copyright 2003 der Autoren:

Reiner Anhorn	Robert Bosch GmbH, Stuttgart
Thomas Barthel	FORBIT e.V./CArO GmbH, Hamburg
Ingmar Carlberg	BIT e.V., Bochum
Armin Elbert	SAP AG, Walldorf
Thomas Glauch	KPMG, Düsseldorf
Ulrich Gleiß	Aventis Pharma Deutschland GmbH, Frankfurt
Jürgen Heck	Brau und Brunnen AG, Dortmund
Georg Hohnhorst	KPMG, Düsseldorf
Werner Hornberger	SAP AG, Walldorf
Andreas Kirk	Ruhrgas AG, Essen
Thomas Müthlein	DMC Datenschutz Management & Consulting GmbH&CoKG, Köln /GDD e.V.
Peter Schiefer	Bayer AG, Leverkusen
Edgar Schmidt	Philip Morris GmbH, München
Hermann-Josef Schwab	SAP AG, Walldorf
Gerhard Voogd	FORBIT e.V./CArO GmbH, Hamburg

Die Verantwortung für den Inhalt tragen die Autoren. Die redaktionelle Bearbeitung liegt bei der SAP AG, Walldorf.

Hinweis: Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechts ist ohne Zustimmung der Urheber unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Autoren des **Leitfaden Datenschutz BW** sind für Kritik, Änderungs- und Ergänzungswünsche dankbar. Dies gilt sowohl für Vorschläge zur Vertiefung der einzelnen Kapitel als auch für die Nennung von Beispielen aus konkreten Prüfungserfahrungen.

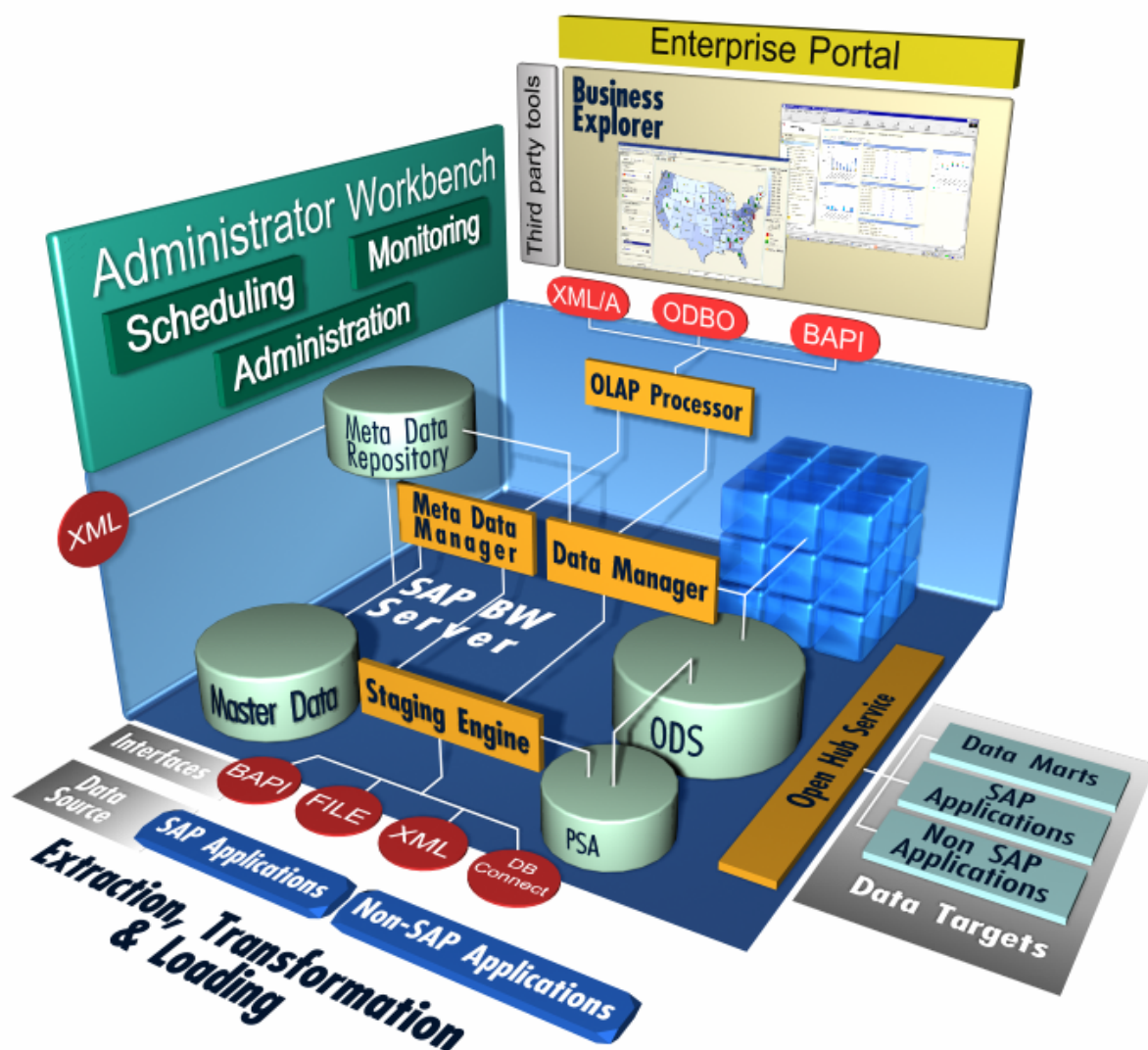
Um dem Leser das Antworten zu erleichtern, ist auf der folgenden Seite ein Antwortformular angefügt:

¹ In der Fassung vom 14.01.2003

0 Einführung

Für die Entscheidungen in den Unternehmen werden heute präzise und aktuelle Informationen aus allen Bereichen des Unternehmens benötigt, aus Marketing, Produktion, Vertrieb, Finanzwirtschaft und Personalwesen. Diese Informationen stecken in vielen verschiedenen Anwendungssystemen und Datenbeständen innerhalb und außerhalb des Unternehmensverbunds. Das Konzept zur Integration und Konsolidierung dieser Daten ist das ‚Data Warehousing‘.

Unter ‚Data Warehousing‘ versteht man eine unabhängige Anwendungsumgebung mit zugehöriger Datenbank, die Daten aus unterschiedlichen Quellen bezieht und flexible Abfragen und Analysen ermöglicht. Das von der SAP angebotene Data Warehouse-System ist das SAP Business Information Warehouse (SAP BW).



Fundament des SAP BW ist ein R/3-Kernel mit dem bekannten Berechtigungskonzept, das um einige Berechtigungsobjekte für die Steuerung der Rechte für Extraktion, Administration, Datenzugriff und um ein Frontend-Tool für den Reportzugriff erweitert wurde. Wie bereits erwähnt, ist eine der Anforderungen an ein Data Warehouse System die Möglichkeit, Daten von vielen unterschiedlichen Plattformen zusammenzufassen. Dazu gibt es im SAP BW

Schnittstellen zu SAP R/3-, R/2- und BW-Systemen sowie zu Non-SAP-Systemen. Auch ein Import von sequentiellen Dateien ist möglich.

Die logisch zusammengehörigen Daten in den Quellsystemen werden als **DataSource** bezeichnet. In einem ersten Schritt werden diese in eine Eingangsablage (**PSA** = Persistent Staging Area) übertragen, wo sie unverändert in relationalen Datenbank-Tabellen gespeichert werden. Mit Übertragungsregeln wird dann festgelegt, wie diese Felder zu InfoObjects und InfoSources zusammengeführt werden sollen.

InfoObjects sind die kleinsten Einheiten des BW. Durch sie werden die betriebswirtschaftliche Auswertungsobjekte wie Kunden, Umsätze, usw. in strukturierter Form abgebildet. Dabei untergliedern sie sich in Merkmale, Einheiten und Zeitmerkmale zur Beschreibung der Art der Werte (z.B. Umsatz mit Dritten in Mio € in 2002) und Kennzahlen (=Werte) wie Beträge, Mengen oder Stückzahlen.

Eine **InfoSource** ist dann die Menge von logisch zusammengehörigen InfoObjects zu einer Art von Geschäftsvorfällen und kann entweder Bewegungs- oder Stammdaten aus einer oder mehreren Quellsystemen umfassen.

Zur langfristigen Ablage werden die Daten anschließend in ODS-Objekte oder InfoCubes fortgeschrieben.

ODS-Objekte (Operational Data Store) stellen eine langlebige Datenablage für konsolidierte und bereinigte Bewegungsdaten auf Belegebene aus einer oder mehreren InfoSources dar. Sie werden in transparenten flachen Datenbank-Tabellen wie in der PSA gespeichert.

Ein **InfoCube** beschreibt einen aus Reportingsicht in sich geschlossenen Datenbestand und ist im BW das zentrale Objekt für mehrdimensionale Reports und Analysen. Er stellt eine aggregierte, leseoptimierte Datenhaltung für performante, multidimensionale Auswertungen dar. Basis-InfoCubes werden mit Daten aus ein oder mehreren InfoSources oder ODS-Objekten versorgt und speichern i.d.R. aggregierte Daten in einer Menge von relationalen Tabellen nach dem Sternschema (mehrere Dimensionen). Bleiben die Bewegungsdaten jedoch außerhalb des BW, spricht man von einem RemoteCube. Die Daten werden nur zur Laufzeit eines Reports auf den RemoteCube im BW verfügbar gemacht.

Näheres zu den Informationsobjekten im BW ist in Kapitel 2.1 zu finden.

Als Werkzeug zur Daten- und Prozessverwaltung steht die Administrator Workbench zur Verfügung. Mit ihr können alle Prozesse zur Datenbeschaffung und Datenverarbeitung im BW gesteuert und überwacht werden. Außerdem liefert sie einen Überblick über alle im BW vorhandenen Informationsobjekte.

Zur Auswertung der Daten steht ein weiteres Werkzeug zur Verfügung, der Business Explorer (BEx), eine Berichts- und Analyseschnittstelle mit vordefinierten Standardberichten und frei definierbaren Listen. Daneben können jedoch auch Tools von Drittanbietern eingesetzt werden.

Generell stellt sich zuerst die Grundfrage, ob und in welcher Form die Verarbeitung personenbezogener Daten in einem BW überhaupt zulässig ist. Es gibt etliche Datenschutzexperten, die dies grundsätzlich für rechtlich problematisch halten.

So können durch die Datenverdichtung z.B. mit statistischen Methoden neue Zusammenhänge „herausgegraben“ und Personen-Profile mit wenig Aufwand erstellt werden. Daneben werden durch die umfassende Datensammlung neue Einblicke im Gesamtzusammenhang z.B. des Unternehmensverbundes ermöglicht. Auch die Zusammenführung der Daten ist nicht unkritisch. So wird die ursprüngliche Zweckbindung z.B. nicht mehr in allen Fällen gegeben sein.

Andererseits ist die Voraussetzung für effektives Data Warehousing der globale Einsatz im Konzern, bei dem i.d.R. nicht die „Tiefenschärfe“ erforderlich ist wie in herkömmlichen Datenbeständen. Dadurch bietet sich hier die Chance, durch entsprechende Maßnahmen den Grundsatz der Datenvermeidung und Datensparsamkeit erfolgreich voranzubringen sowie oftmals einen Personenbezug ganz zu vermeiden.

D.h. Data Warehouse Systeme erhöhen damit grundsätzlich auf der einen Seite die Bedrohung der Persönlichkeitsrechte und können auf der anderen Seite gleichermaßen auch deren Schutz verbessern. Die Risiken in Grenzen zu halten und den Schutz zu stärken, wollen wir mit unseren folgenden Ausführungen erreichen.

1 Rechtliche Anforderungen an ein SAP Business Warehouse (BW)

Das Datenschutzrecht spricht ein grundsätzliches Verbot der Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus und erlaubt die Datenverarbeitung nur, wenn die im Datenschutzrecht definierten Voraussetzungen erfüllt sind (Verbot mit Erlaubnisvorbehalt). So ist die Verarbeitung personenbezogener Daten nur mit einer entsprechenden Rechtsgrundlage möglich. Im Wesentlichen zählen hierzu die Einwilligung, Betriebsvereinbarungen und vertragliche Regelungen.

Im Sinne des Datenschutzrechts findet im Business Warehouse (BW) eine Nutzung der vorgelagerten Daten statt, mit Ausnahme der Auswertungserstellung erfolgen alle anderen Prozesse der Datenverarbeitung in den vorgelagerten operativen Systemen.

Das bedeutet gleichzeitig, dass die Frage der Zulässigkeit der Erhebung und Verarbeitung der Daten in der Regel schon im Vorfeld bei den operativen Systemen geklärt werden muss. Für die dort eingesetzten SAP-Systeme sind die Hinweise im *Leitfaden Datenschutz für SAP R/3* zu beachten.

Für das BW-System ist damit besonders die Frage zu klären, in wie weit die Verarbeitung der übernommenen Daten noch für die Erfüllung der ursprünglichen Zwecke notwendig ist. Vielfach wird mit dem Einsatz des BW ein Eigeninteresse des Unternehmens unabhängig vom ursprünglichen Erlaubnistatbestand, z. B. Vertragsbeziehung, verfolgt (Zweckänderung). Hierbei ist zu beachten, dass bei Wegfall der Zweckbindung eine unzulässige Vorratsspeicherung vorliegt. Dies ist insbesondere dann der Fall, wenn in dem BW-System zunächst personenbezogene Daten gesammelt und die Auswertungen erst in der Zukunft festgelegt werden sollen.

In vielen Fällen wird der Zugriff auf personenbezogenen Daten nicht benötigt, das SAP BW wird zur Optimierung der betriebliche Prozessketten verwendet, ohne dass hierfür die Auswertung von Daten mit Personenbezug erforderlich ist.

Wenn das BW-System nur zur Entlastung des operativen Systems eingesetzt wird, kann sich die Prüfung durch den Datenschutzverantwortlichen im Unternehmen auf das Berechtigungskonzept beschränken. Voraussetzung ist, dass die Zwecke, der Datenumfang, die Speicherdauer und der zugriffsberechtigte Personenkreis nicht ausgedehnt werden.

Sieht man von Systemen im oben genannten Sinne ab, die z.B. nur hinter ein R/3-System gestellt werden, um über Reporting-Tools einfachere Auswertungen zu ermöglichen, ist das Zusammenführen personenbezogener Daten aus unterschiedlichen Systemen wegen der Zweckbindung rechtlich anders zu bewerten.

Als Zulässigkeitskriterium bleibt neben der Schaffung eines neuen Erlaubnistatbestandes, z. B. durch Einwilligung der Betroffenen, nur die Anonymisierung. Liegt eine eindeutige Anonymisierung aller personenbezogenen Daten vor, d.h. es kann nicht mehr auf die Einzelperson rückgeschlossen werden, sind die datenschutzrechtlichen Bestimmungen nicht mehr anwendbar.

Bei einer Pseudonymisierung² hingegen bleibt das Datenschutzrecht anwendbar, da die Daten zwar zunächst für den Betrachter anonym sind, aber der zugehörige Personenbezug jederzeit wieder hergestellt werden kann. Entscheidend ist hier, wer im Besitz der Zuordnungstabelle ist und damit die Möglichkeit hat, den direkten Personenbezug wieder herzustellen³.

In allen Fällen sollte der Datenschutzverantwortliche rechtzeitig vor Einführung eines BW-Systems zur Klärung der komplexen datenschutzrechtlichen Tatbestände einbezogen werden. Gegebenenfalls ist sogar eine Vorabkontrolle durchzuführen.

Zur Bewertung des BW-Systems ist also vor der Prüfung zu klären, ob personenbezogene, pseudonyme oder anonyme Daten an das BW übergeben werden und welche dieser drei Datenklassen in der Basis vorgehalten bzw. über die InfoCubes ausgewertet werden (siehe Beispiel eines BW-HR-Systems Abb. 1). Weitere Anforderungen können sich ergeben, wenn das BW bzw. die vorgeschalteten Systeme durch einen Dienstleister betrieben werden (siehe Abb. 2).

² EU-Richtlinie

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr fordert Datenvermeidung und Datensparsamkeit.

Erwägungsgrund 26

Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Die Verhaltensregeln im Sinne des Artikels 27 können ein nützliches Instrument sein, mit dem angegeben wird, wie sich die Daten in einer Form anonymisieren und aufbewahren lassen, die die Identifizierung der betroffenen Person unmöglich macht.

Artikel 6

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten ...

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen; ...

e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiter verarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht.

BDSG

§ 3 BDSG, Weitere Begriffsbestimmungen

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

§ 3a BDSG, Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

³ Diese Auffassung ist derzeit umstritten, da die Pseudonymisierung einerseits als Mittel der Datenvermeidung und Datensparsamkeit im BDSG besonders empfohlen wird (§ 3a BDSG). Dies ist nach dem Wortlaut des BDSG z.Zt. allerdings mit keinerlei Verarbeitungserleichterungen verbunden.

Hiergegen wenden sich neuere Stimmen wie Rossnagel/ Scholz⁴ oder der Gutachterausschuss zur „Modernisierung des Datenschutzrechts, insbesondere grundlegende Novellierung des Bundesdatenschutzgesetzes“. Zu Recht stellen sie darauf ab, ob die Zuordnung bei der konkreten Verarbeitung möglich und gewollt ist. Ist dies nicht der Fall, z. B. wenn die Zuordnungstabelle⁵ in einer anderen Abteilung unter Verschluss gehalten wird, sind die Daten für den Verwender mit den oben dargestellten Folgen anonym.

Abbildung 1:

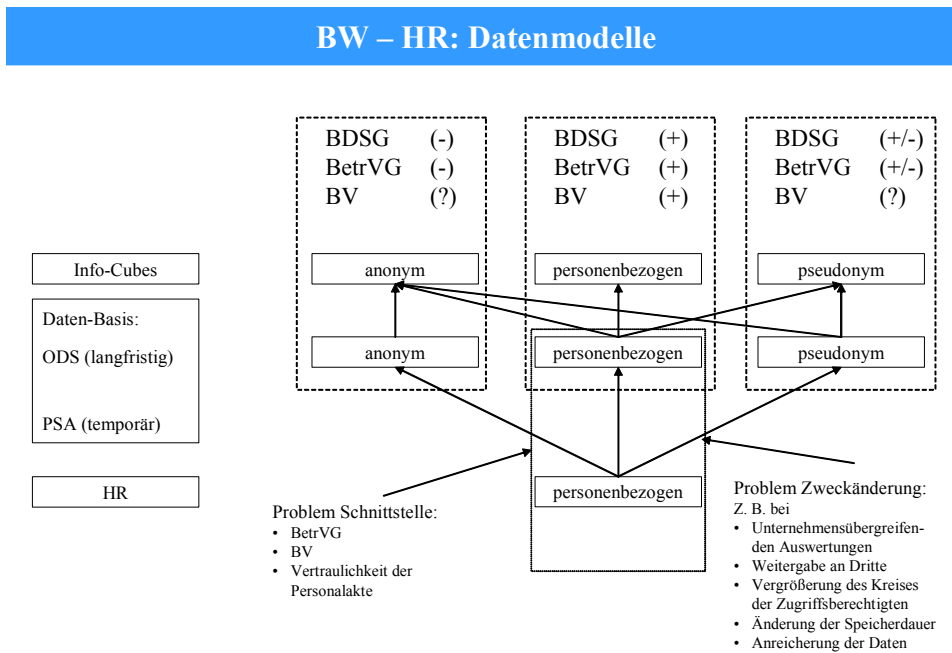
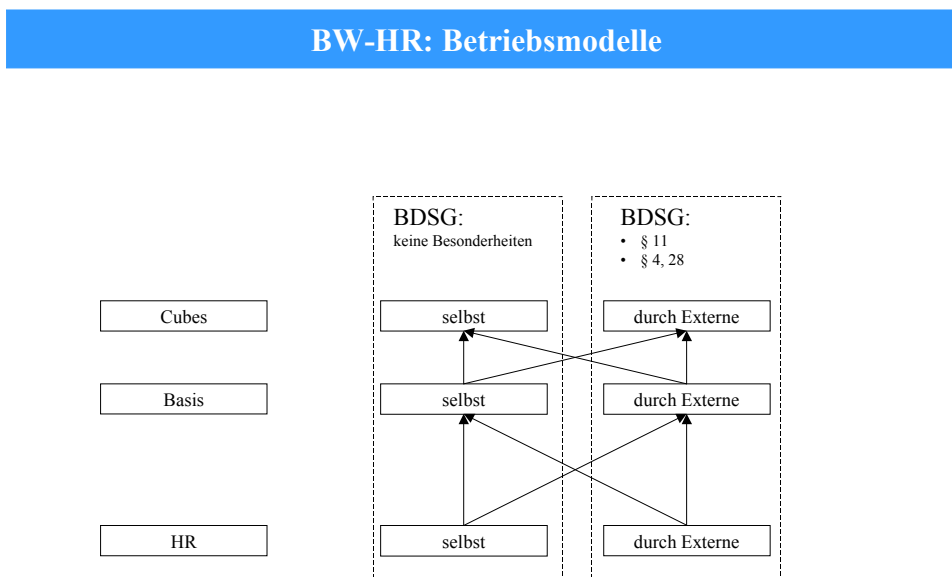


Abbildung 2:



Prüfungsfelder:

Damit ergeben sich für den Datenschutzverantwortlichen im wesentlichen die folgenden drei Prüfungsfelder:

- a) Datenübergabe ans BW
- b) Vorhalten von Daten in der Basis
- c) Art und Umfang der von den InfoCubes bereitgestellten Sichten und Auswertungen

zu a) Datenübergabe ans BW

- Selbst wenn an das BW nur anonymisierte Daten übergeben werden und das Datenschutzrecht hierauf und auf den Umgang mit diesen Daten im BW keine Anwendung findet, bleibt dennoch zu prüfen, ob bestehende Betriebsvereinbarungen oder besondere gesetzliche Regelungen die anonyme Weitergabe und Nutzung reglementieren.
- Sollen personenbezogene oder pseudonymisierte Daten an das BW weitergegeben werden, so ist bereits im Vorfeld der Datenübergabe zu prüfen, ob
 - o Rechtsvorschriften (besondere Geheimhaltungspflichten z. B. ärztliche Schweigepflicht, Vertraulichkeit der Personalakte oder Fernmelde-, Bank-, Steuergeheimnis) oder
 - o im Bereich der Personaldatenverarbeitung bestehende Betriebsvereinbarungen oder
 - o Bestimmungen des Datenschutzrechts

vorhanden sind, die die Übergabe einschränken oder gar verbieten.

Eine solche Prüfung ist insbesondere erforderlich, wenn das BW-System nicht nur zur Entlastung des operativen Systems eingesetzt wird, sondern z. B.

- o die Zwecke,
- o der Datenumfang,
- o die Speicherdauer,
- o die Auswertungsmöglichkeiten oder
- o der zugriffsberechtigte Personenkreis mit entsprechenden Berechtigungen
- o ausgedehnt werden.

zu b) Vorhalten von Daten in der Basis

Die Datenbasis ist zu unterscheiden in PSA und ODS-Objekt (s. Kapitel 0).

Die PSA dient im wesentlichen der kurzfristigen Zwischenspeicherung der ins BW geladenen Daten, bevor sie in der endgültigen BW-Datenbasis (ODS-Objekt) abgelegt werden.

Damit sind insbesondere für die PSA technisch/organisatorische Maßnahmen und im Hinblick auf die kurzfristige Speicherung der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten. Das führt in der Regel dazu, dass die Daten nach erfolgreichem Hochladen in die ODS-Objekte in der PSA zu löschen sind.

Bei den ODS-Objekten ist darüber hinaus insbesondere die Speicherdauer im Hinblick auf die Geschäftszwecke und die damit verbundene Anforderlichkeit zu beachten. Die Anforderlichkeit ergibt sich hierbei aus den mit dem BW verfolgten Zwecken. Dabei ist in diesem Zusammenhang auch regelmäßig der Umfang der gespeicherten Daten zu überprüfen.

zu c) Art und Umfang der von den InfoCubes bereitgestellten Sichten und Auswertungen

Bei der Prüfung stehen folgende datenschutzrechtliche Grundprinzipien im Vordergrund:

- Zweckbindung
- Klärung der Reichweite der vorhandenen Rechtsgrundlage der operativen Systeme für das BW
- Schaffung neuer Rechtsgrundlagen, z. B. durch Einwilligung oder vertragliche Regelungen (s. § 28 Abs. 1 BDSG)
- Transparenz der Datenverarbeitung
- Qualität (Datenintegrität und –konsistenz)

2 SAP-Fakten und Datenschutzaspekte

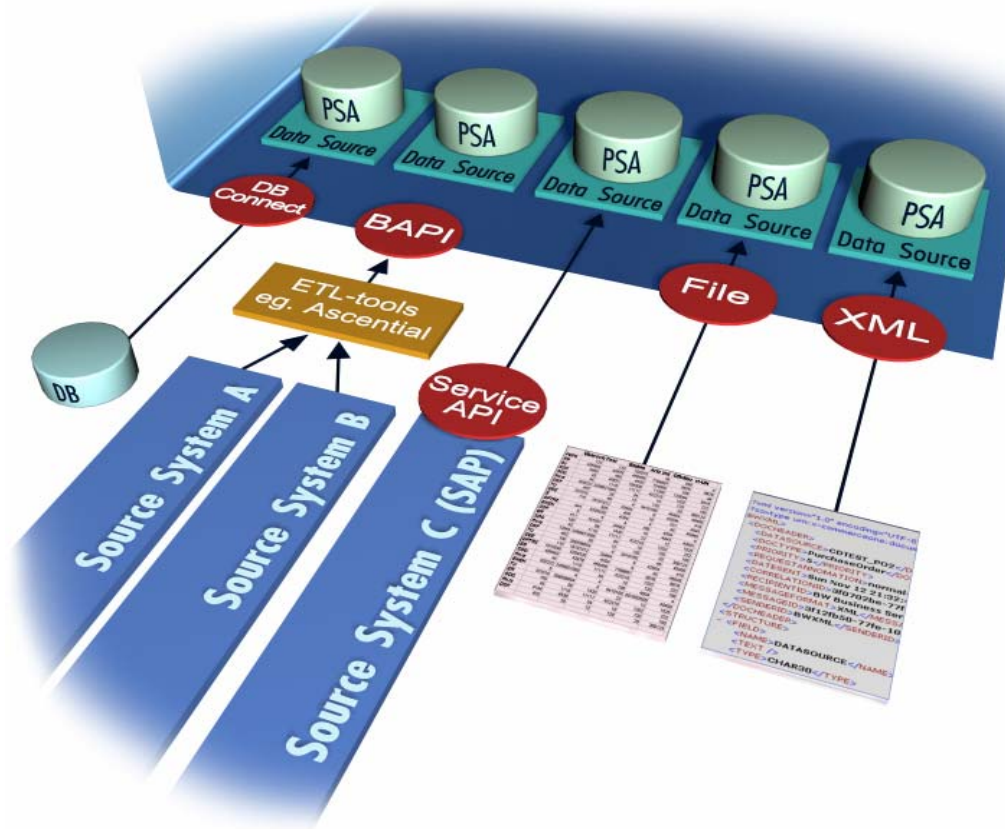
Im Unterschied zu einem reinen R/3-System melden sich die Endbenutzer in der Regel nicht direkt im Business Warehouse an, sondern erhalten über ein Portal oder ein Frontend Tool den benötigten Zugang, um Reports ausführen bzw. ändern zu können. Die vom R/3 bekannte Anmeldung über den SAPGUI ist nur für die BW-Administration notwendig, kann aber auch vom Enduser erfolgen.

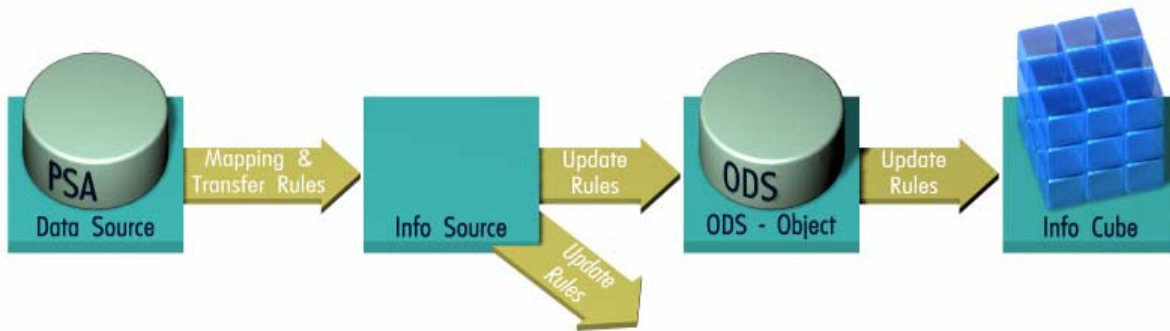
Bei der Installation des SAP Frontendtools werden Analyser, Browser, Download Scheduler, Formatted Reporting, Query Designer und der Web Application Designer installiert. Die Berechtigungsprüfung erfolgt im BW-System. Bei entsprechender Berechtigung besitzt der User folglich nicht nur Leseberechtigung, sondern auch die Möglichkeit, Reports zu verändern.

2.1 Datenbereitstellung und Datenhaltung

Das SAP BW System empfängt Daten aus einem oder mehreren operativen Systemen, wobei es sich hierbei um SAP (R/3, CRM etc.)- als auch SAP-fremde Systeme handeln kann. Allgemein werden diese Systeme als Quellsysteme bezeichnet.

Die aus den Quellsystemen hochgeladenen Daten werden im SAP BW in eine für das Unternehmen aussagefähige Form gebracht, d.h. sie werden zu Informationen aufbereitet. Den Datenfluss veranschaulichen die nachstehenden Grafiken.





In der Administrator Workbench des SAP BW Systems sind zahlreiche Funktionen enthalten, um sich einen umfassenden Überblick über die verwendeten Quellsysteme und die im SAP BW definierten Objekte zu verschaffen.

Besteht für den Prüfer die Notwendigkeit, die gesamte Datenstruktur einschließlich des Datenflusses näher zu analysieren, stehen Werkzeuge der Administrator Workbench (Transaktion RSA1) zur Verfügung. Da diese über umfassende Rechte verfügen (z.B. Änderungsberechtigung), kann eine Prüfung nur in Zusammenarbeit mit der Administration erfolgen.

Um eine Auflistung der verwendeten Quellsysteme zu erhalten, ist im Navigationsmenü der Administrator Workbench der Auswahlbutton „Modellierung“ anzuklicken. Anschließend wählen Sie den Eintrag „Quellsysteme“ aus.

Menüpfad:

BW Administration -> Administrator Workbench -> Modellierung -> Quellsysteme

2.1.1 DataSource

Das Datenangebot eines Quellsystems wird in SAP BW durch DataSources in betriebswirtschaftlich abgeschlossene Bereiche untergliedert. Diese Bereiche stellen quellsystemabhängige DataSource-Typen dar, die zur Übertragung von Stamm- und Bewegungsdaten genutzt werden. Hierbei werden zwei Feldstrukturen voneinander unterschieden:

- Extraktionsstruktur
- Transferstruktur

Die Extraktstruktur einer DataSource enthält die Menge der Felder des Quellsystems, die für den Datenladeprozess angeboten werden. Die Transferstruktur stellt eine Auswahl der Felder der Extraktstruktur eines Quellsystems dar. Mit Hilfe eines speziellen Programms, dem sog. Extraktor, werden die Inhalte der Felder der Extraktstruktur an die Transferstruktur übergeben. Hierüber werden die Daten vom Quellsystem in das SAP BW übertragen.

Um die DataSources eines bestimmten Quellsystems zu ermitteln, ist im Navigationsmenü zunächst der Auswahlbutton „Modellierung“ anzuklicken. Anschließend ist der Eintrag „Quellsysteme“ auszuwählen. Nach Doppelklick auf den Namen des Quellsystems, werden die zu diesem Quellsystem definierten DataSources im Anzeigebereich der Administrator Workbench aufgelistet.

Menüpfad:

BW Administration -> Administrator Workbench -> Modellierung

Bei der Prüfung des SAP BW Systems kann es sich als hilfreich erweisen, die Extraktionsstruktur einer DataSource zu ermitteln, d.h. um festzustellen, welche Felder eines Quellsystems dem SAP BW angeboten werden. Hierzu wählen Sie im Navigationsmenü den Eintrag „Modellierung“ aus und klicken anschließend auf „Quellsysteme“. Im Anzeigebereich wählen Sie nun die zu untersuchende DataSource mit der rechten Maustaste aus und klicken im dann erscheinenden Pop-up-Fenster auf „Objektübersicht“. In einem neuen Fenster wird die Übersicht der von einer DataSource angebotenen Felder angezeigt und zusätzlich die Namen der InfoObjects an die Daten dieser Felder übergeben werden.

Im Quellsystem (sofern es sich um ein R/3 System handelt) können diese Information über die Funktion „Generische DataSource bearbeiten“ (Transaktion RSO2) bzw. „Nachbearbeitung von DataSources“ (Transaktion SBIW) ermittelt werden.

Transaktion:

SPRO -> Button SAP Referenz-IMG drücken

Menüpfad:

Integration mit anderen SAP Komponenten -> Datenübertragung in das Business Information Warehouse -> Generische DataSource bzw. Nachbearbeitung von DataSources

Eine Auflistung aller DataSources erhält man auch durch die Auswahl „Metadata Repository“ im Navigationsmenü. Anschließend ist im Anzeigebereich der Eintrag „DataSource / FileSource“ auszuwählen.

Menüpfad:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.1.1 Persistent Staging Area

Die Persistent Staging Area (PSA) ist die Eingangsablage für Daten aus den Quellsystemen im SAP BW. Dort werden die angeforderten Daten unverändert zum Quellsystem gespeichert.

Die Speicherung der Daten erfolgt in relationalen Datenbanktabellen (PSA-Tabellen) des SAP BW deren Aufbau der Transferstruktur entspricht und zusätzliche Systemfelder enthält. Bei Änderungen an der Transferstruktur wird eine neue Version der PSA-Tabelle angelegt. Das bisherige Datenformat bleibt daher unverändert, d.h. es erfolgen keinerlei Verdichtungen oder Transformationen.

Die in den PSA-Tabellen gespeicherten Daten können manuell modifiziert werden. Vor allem für die Sicherstellung der Datenqualität und des korrekten Datenladeprozesses erweist sich die PSA als zusätzliche Kontrollinstanz.

Vor der Übertragung in die InfoSource besteht die Möglichkeit, Bewegungs- und Stammdaten in der PSA zwischenspeichern, d.h. die PSA kann optional als Zwischenspeicher für operationale Daten genutzt werden. Sie ist allerdings nur als zeitlich begrenzter Zwischenspeicher und nicht für eine permanente Speicherung der Daten gedacht.

Menüpfad:

BW Administration -> Administrator Workbench -> Modellierung -> PSA

2.1.1.2 Metadata Repository

Die Beschreibung der Quelldaten (Stamm- und Bewegungsdaten) erfolgt mit Hilfe sog. Metadaten (z.B. Herkunft, Historie, und andere Aspekte der Daten). SAP BW kennt drei Klassen von Metadaten:

- technische Daten
- Nutzerdaten und
- betriebswirtschaftliche Daten (Unternehmensdefinitionen).

Technische Metadaten beschreiben die technischen Eigenschaften wie z.B. Feldlänge, Datentyp. Nutzer-Metadaten enthalten Informationen über die Autorisierung. Unternehmensdefinitionen liefern in SAP BW das notwendige Verständnis für die Geschäftsterminologie. Hierüber werden beispielsweise spezielle Leistungskennzahlen (Key Performance Indicators) festgelegt.

SAP BW ist mit einem zentralen **Metadata Repository** ausgestattet, das zu integrierten, konsistenten und korrekten Metadaten beiträgt und das die Wiederverwendung von Metadaten im gesamten Unternehmen ermöglicht. Mit dem Metadata-Repository werden zentral alle SAP BW Meta Objekte und deren Verknüpfungen zueinander verwaltet. Der Metadaten **Repository Browser** ermöglicht dem Administrator einen schnellen Zugriff auf die Metadaten aller SAP-BW-Objekte.

Das Metadata Repository kann nach technischen Namen, beschreibenden Texten usw. durchsucht werden. Außerdem können Metadaten zwischen verschiedenen Systemen ausgetauscht, HTML-Seiten exportiert sowie grafische Darstellungen zu den Objekten angezeigt werden.

Menüpfad:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.2 InfoObjects

Die kleinsten Informationsbausteine (= Felder) des SAP BW werden als InfoObjects bezeichnet. Sie sind über ihren technischen Namen eindeutig identifizierbar. Es handelt sich hierbei um betriebswirtschaftliche Auswertungsobjekte, die Daten über Kostenstellen, Mitarbeiter, Kunden, Umsätze usw. enthalten können.

InfoObjects haben im wesentlichen drei Funktionen:

Als Bestandteil des Metadaten Repository tragen sie die technischen und fachlichen Informationen der Stamm- und Bewegungsdaten im SAP BW. Sie werden systemweit zum Aufbau von Tabellen und Strukturen eingesetzt, wodurch die Informationen im SAP BW in strukturierter Form abgebildet werden können. Darüber hinaus werden sie für die Definition von Berichten verwendet, um Stamm- und Bewegungsdaten auszuwerten.

InfoObjects werden nach Kategorien, d.h. entsprechend der Art der durch sie repräsentierten Daten, wie Merkmale und Kennzahlen klassifiziert. Merkmale sind z.B. Produkt, Kundentyp, Finanzjahr, Zeitraum oder Region die dazu dienen, Auswertungsgruppen für eine Analyse zu erstellen. Kennzahlen können Werte oder Mengen wie Verkaufserlöse, Fixkosten, Verkaufsmenge oder Personalbestand sein.

Über die Funktionen der Administrator Workbench erhält man eine technische Beschreibung der InfoObjects. Hierzu ist die Auswahl „Modellierung“ im Navigationsmenü zu treffen. Im Anzeigebereich werden daraufhin die InfoObjects nach InfoAreas sortiert aufgelistet. Durch Doppelklick auf das gewünschte InfoObject gelangt man zur Detailanzeige des InfoObjects.

Menüpfad:

BW Administration -> Administrator Workbench -> Modellierung -> InfoObjects

Nach Auswahl des „Metadata Repository“ im Navigationsmenü und anschließendem Mausklick auf den Eintrag „InfoObject“ wird eine Liste der aktivierten InfoObjects angezeigt. Eine nach Bereichen sortierte Auflistung der InfoObjecte erhält man auch durch Auswahl des Eintrags „InfoObjectCatalog“.

Menüpfad:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.3 InfoSource

Eine InfoSource ist eine Menge von zusammengehörigen InfoObjects, die alle verfügbaren Informationen eines Geschäftsprozesses enthalten (z.B. Kostenstellenrechnung). Die Struktur, in der diese Informationen abgelegt sind, heißt **Kommunikationsstruktur**. Sie ist die technische Realisierung der InfoSource. Die Kommunikationsstruktur ist im Gegensatz zur Transferstruktur quellsystemunabhängig, da sie aus verschiedenen Quellsystemen versorgt werden kann.

Mit Hilfe der InfoSource wird der systemübergreifende Transport von Daten zwischen Quellsystemen und dem SAP BW ermöglicht. Datenanforderungen an das Quellsystem erfolgen pro InfoSource und Quellsystem. InfoSources können ebenso wie die zugrunde liegenden InfoObjects entweder Bewegungsdaten oder Stammdaten (Attribute, Texte und Hierarchien) bereitstellen, wobei der Aufbau von InfoSources für Bewegungs- und Stammdaten nahezu identisch ist.

Nachdem die Daten des Quellsystems in der PSA abgelegt wurden, können sie von dort direkt in den Datenspeicher des Operational Data Store's oder direkt in InfoCubes geladen werden. Dies wird normalerweise nur dann vorkommen, wenn keine Notwendigkeit zum Bereinigen, Transformieren oder Konsolidieren, d.h. zur Aufbereitung der aus dem Quellsystem übernommenen Daten besteht.

Im Regelfall werden die im SAP BW System empfangenen Daten aber mittels **Konvertierungsregeln/Übertragungsregeln** aufbereitet und an die Kommunikationsstruktur übergeben. Die Übertragungsregeln legen fest, welche Felder der Transferstruktur in welche Felder der Kommunikationsstruktur zu übertragen sind, bzw. welche Felder den entsprechenden InfoObjects einer InfoSource zuzuordnen sind. Konvertierungsregeln werden benötigt, wenn Daten bei Aktionen wie Datum-/Zeit-Konvertierungen, Zeichenfolgenoperationen usw. in die benötigte Geschäftslogik übertragen werden.

Über die Kommunikationsstruktur werden die Daten im SAP BW dann zur weiteren Verwendung angeboten.

Menüpfade:

BW Administration -> Administrator Workbench -> Modellierung -> InfoSource

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.4 Operational Data Store

Der Operational Data Store (ODS) wird verwendet, um granulare Daten abzufragen, die häufig aktualisiert werden. Ein Operational Data Store-Objekt (ODS-Objekt) dient der Ablage von konsolidierten und bereinigten Daten (z.B. Bewegungsdaten oder Stammdaten) auf Belegebene (atomarer Ebene). Es beschreibt einen konsolidierten Datenbestand aus einer oder mehreren InfoSources.

Die Daten der ODS-Objekte werden in transparenten Datenbanktabellen gespeichert. Sie können mit Hilfe eines Delta-Updates in InfoCubes oder anderen ODS-Objekten aktualisiert werden.

Info Objects, ODS-Objekte und InfoCubes werden in SAP BW auch unter dem Oberbegriff „InfoProvider“ aufgeführt. Die ODS-Objekte findet man deshalb im Navigationsmenü durch Auswahl „Modellierung“/„InfoProvider“. Zu den InfoProvidern zählen auch InfoSets, RemoteCubes und MultiProvider.

Menüpfad:

BW Administration -> Administrator Workbench -> Modellierung -> InfoProvider

Zur Anzeige und weiteren Analyse der ODS-Objekte gelangt man auch durch Auswahl des „Metadata Repository“ und anschließendem Mausklick auf den Eintrag „ODS-Objekt“ im Anzeigebereich.

Menüpfad:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.5 InfoCube

InfoCubes sind die zentralen Objekte des multidimensionalen Datenmodells (Datenwürfel) im SAP BW. Sie umfassen eine logisch zusammengehörende Menge an InfoObjects.

Ein InfoCube beschreibt aus Reporting-Sicht einen in sich geschlossenen Datenbestand eines betriebswirtschaftlichen Bereichs. Der hierüber repräsentierte Datenbestand (Bewegungsdaten werden ausschließlich in InfoCubes abgespeichert) kann mit unterschiedlichen Frontend-Tools aus verschiedenen Geschäftsperspektiven wie z.B. geografische Region oder Art des Vertriebskanals ausgewertet werden.

Beim Erstellen eines mehrdimensionalen InfoCubes werden Fortschreibungsregeln angelegt, die immer über eine Kombination aus InfoCube und InfoSource definiert werden. Daher kann eine InfoSource mehrere InfoCubes fortschreiben, es ist aber auch möglich, dass eine InfoCube mit mehreren InfoSources verbunden ist.

InfoCubes finden Sie ebenso wie ODS-Objekte unter dem Oberbegriff „InfoProvider“. Wählen Sie im Navigationsmenü „Modellierung“ und anschließend den Eintrag „InfoProvider“ aus.

Menüpfad:

BW Administration -> Administrator Workbench -> Modellierung -> InfoProvider

Zur Anzeige und weiteren Analyse der InfoCubes gelangt man auch über das „Metadata Repository“. Klicken Sie im Anzeigebereich des Metadata Repository auf den Eintrag „InfoCube“.

Menüpfad:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.5.1 Fortschreibung

SAP BW unterstützt zwei verschiedene Fortschreibungsarten wie Daten in das SAP BW geladen werden können. Das Full-Update extrahiert immer alle Daten der Felder einer Transferstruktur. Die zweite Fortschreibungsart, das Delta-Update, extrahiert nur die Daten, die sich seit dem letzten Ladevorgang verändert haben oder neu hinzugekommen sind. Gerade bei großen Datenmengen ist natürlich ein Delta-Update Verfahren geeignet, um Daten nicht mehrmals in das SAP-BW laden zu müssen. Mit Hilfe sog. InfoPackages können gezielte Teilmengen der in der DataSource definierten Daten beschrieben werden. Durch präzise Selektionsparameter (Auswahlkriterien, DataSource-Parameter, Aktualisierungsmodi und Planungsspezifikationen) wird festgelegt, welche Bewegungsdaten oder Stammdaten (z.B. nur Kostenrechnungskreis 001 in Periode 10.2000“) einer DataSource angefordert werden.

Eine Auflistung aller definierten Fortschreibungsregeln erhalten Sie über das „Metadata Repository“. Im Anzeigebereich ist anschließend der Eintrag „Fortschreibungsregeln“ durch Mausclick auszuwählen.

Menüpfad:

BW Administration -> Administrator Workbench -> Metadata Repository

Zur Anzeige der Fortschreibungsregeln eines InfoObjekts, InfoCubes und ODS-Objekts gelangt man durch Auswahl des jeweiligen Objekts. Gehen Sie hierzu wie im jeweiligen Kapitel beschrieben vor.

2.1.5.2 Sternschema

Beim Anlegen eines InfoCubes werden die Merkmale zu Dimensionstabellen zusammengefasst und um eine zentrale Faktentabelle, die Kennzahlen enthält, positioniert. Dieses Schema wird Sternschema genannt. Es klassifiziert zwei Gruppen von Daten: Fakten (z.B. Umsatz, Menge) und Dimensionsattribute (z.B. Kunde, Material, Zeit). Die Fakten stehen im Mittelpunkt der Analyse des Unternehmensgeschehens.

SAP BW arbeitet mit einem erweiterten Sternschema, in dem Stammdaten (über Attribute, Hierarchien und Texte) in separaten Tabellen gespeichert werden können, die von den InfoCubes gemeinsam genutzt werden.

2.1.5.3 Aggregat

Zur Reduzierung des Datenvolumens pro Abfrage ist es möglich, Aggregate zu implementieren. Ein Aggregat ist eine materialisierte, aggregierte Sicht auf die Daten oder Teilmengen von Daten eines InfoCubes. In einem Aggregat wird der Datenbestand eines InfoCubes in verdichteter Form redundant und persistent auf der Datenbank gespeichert.

Ebenso wie Datenbankindizes verbessern auch Aggregate die Performance, ohne dass der Endanwender in diese Vorgänge eingreifen bzw. Kenntnisse über die Ausführung dieses Vorganges haben muss.

Aggregate können für:

- Merkmale
- Attribute und
- Hierarchien

erstellt werden.

2.1.6 Business Content

Der Business Content gehört zum Lieferumfang von SAP BW. Bei diesen Inhalten handelt es sich um eine reichhaltige Sammlung vorkonfigurierter Informationsmodelle. Dazu zählen Extraktoren, mehrere tausend InfoObjects und einigen hundert InfoCubes und ODS-Objekte. Zudem gehören auch vordefinierte Templates für Berichte und Analysen mit allen zugehörigen technischen und geschäftlichen Definitionen zum Business Content. Einige dieser Objekte sind branchenspezifisch, einige sind bereichs- bzw. funktionspezifisch, wie zum Beispiel für Customer Relationship Management und Supply Chain Management. Ebenfalls Teil dieses Konzepts sind die so genannten technischen Inhalte (z.B. Informationsmodelle), mit denen der Administrator feststellen kann, inwieweit einzelne Objekte in SAP BW genutzt werden.

Mit dem Business Content soll dem Unternehmen ein Ausgangspunkt für die Datenmodellierung und -analyse bereitgestellt werden. Gegebenenfalls kann das Unternehmen den Business Content unverändert übernehmen, es kann neue Inhalte erstellen oder die Business-Content-Objekte an die speziellen Erfordernisse anpassen. Letzteres ist in vielen Fällen effizienter als das Erstellen eines komplett neuen Objekts. Um die individuellen InfoObjects von ausgelieferten Objekten unterscheiden zu können, beginnen SAP-InfoObjects mit der Ziffer 0 und kundeneigene InfoObjects mit einem Buchstaben von A bis Z.

Kundennamensraum

Um zu vermeiden, dass es Namenskonflikte mit den lokalen Objekten der Kunden gibt, muss der Kunden-Content in einem eigenen Namensraum entwickelt werden. Sie können entweder einen eigenen (bei SAP zu beantragenden) Namensraum oder einen vereinbarten Teilbereich des Standard- Kundennamensraumes (A* bis Z*) verwenden.

Tabelle SAP-Namensraum

	SAP Namensraum	Beispiel	Tabelle im ABAP Dictionary
InfoObjekte	0xx_	0ME_CITY01 Ortsname	

	SAP Namensraum	Beispiel	Tabelle im ABAP Dictionary
		0MATERIAL	/BI0/PMATERIAL
InfoObjekte	0xxx_	0CRM_PAYERP Regulierer	
InfoArea	0nn_	0CO OM CCA	
Infocube	0nnn_Cnn	0CCA_C01	
Multicube	0nnn_MCnn	0CCA_MC01	
Virtual Cube	0nnn_VCnn	0CCA_VC01	
ODS Object	0nnn_DSnn 0nnn_Onn	0WEB_O01	/BI0/AWEB_O0100
Query	0nnn_Cnn Qnnn	0CCA_C01 Q0003	
Query_View	0nnn_Cnn Qnnn Vnn	0CCA_C01 Q0003 V01	

0xx_ wo xx zwei Charakter Abkürzungen für die IBU

0xxx_ wo xxx drei Charakter Abkürzungen für die Softwarekomponente

Industrie Lösungen

Abkürzungen	Industry Business Unit (IBU)
AD	Aerospace and Defense
AF	Apparel and Footware Solution
AU	Automotive
BA	Banking
CH	Chemicals
CP	Consumer Products
EN	Engineering & Construction
HC	Healthcare
HT	High Tech
IS	Insurance
ME	Media
MP	Mill Products

Abkürzungen	Industry Business Unit (IBU)
OI	Oil & Gas
PH	Pharmaceuticals
PU	Public Sector
RT	Retail
SP	Service Provider
TE	Telecommunications
TA	Transportation
UC	Utility Companies

Beispiel: Ein spezielles Attribut der *Retail-Materialwirtschaft* benötigt folgendes InfoObject:
ORT_MAT

Softwarekomponenten (Beispiele)

Abkürzung	Software Komponenten
APO	Advanced Planner and Optimizer
MSA	Mobile Sales
CRM	Customer Relation Management
SEM	Strategic Enterprise Management
EBP	Enterprise Buyer (Procurement)
FRE	Forecast & Replenishment Engine
MAP	Merchandising & Assortment Planning
RPA	PIPE (PointOfSales Inound Processing Engine)

Beispiel: Ein spezielles Attribut der *Mobile Sales* benötigt folgendes InfoObjekt **0MSA_CUST**.

2 Einführungsmethoden

Grundsätzlich gibt es zwei verschiedene Vorgehensweisen bei der Einführung eines BW. Zum einen handelt es sich um die klassische Einführungsmethode entlang von Vorgehensmodellen an Hand von ASAP, bzw. jetzt Solution Manager. Zum zweiten gibt es das Vorgehen,

durch Untersuchung und ggf. Abänderung von Vorlagen – im BW Zusammenhang Business Content genannt.

2.2.1 ASAP und Solution Manager

Die SAP Empfehlungen zur Einführung des Business Information Warehouse folgten früher dem allgemeinen ASAP Modell für mySAP Komponenten. Künftig ersetzt der Solution Manager das ASAP Modell. Das ASAP Modell, bzw. der Solution Manager enthält neben dem allgemeinen Vorgehensmodell auch spezielle Beschleuniger (Accelerator) für BW. Das folgende Kapitel befasst sich schwerpunktartig mit den Aktivitäten im Vorgehensmodell, die einen Bezug zu den Anforderungen des Datenschutzes haben. Der betriebliche/behördliche Datenschutzbeauftragte sollte sich bei seiner Befassung mit dem einzuführenden Business Information Warehouse diese Aufgaben besonders vornehmen und gegebenenfalls die für die konkrete Einführung relevanten Aspekte mit dem Projekt/Unterprojekt verhandeln. Wenn eine Vorabkontrolle notwendig ist, müssen diese Punkte im einzelnen vor Produktivsetzung des BW Systems untersucht werden.

Das ASAP Vorgehensmodell unterscheidet allgemein die im folgenden aufgelisteten fünf Hauptphasen: Projektvorbereitung (1), Business Blueprint (2), Realisierung (3), Produktionsvorbereitung, bzw. Final Preparation (4) und GO-LIVE und Support (5). Der Schwerpunkt der inhaltlichen Befassung des Datenschutzbeauftragten mit dem BW Einführungsprojekt liegt dabei unzweifelhaft auf den Phasen des Business Blueprint und der Realisierung. Im folgenden sollen die Hauptfragen des Datenschutzes in den einzelnen Phasen angedeutet werden:

2.2.1.1 Projektvorbereitung

Im Rahmen der *Projektvorbereitung* gilt es zu klären, wie der Datenschutzbeauftragte in das Projekt eingebunden wird. Dies kann von der Mitgliedschaft im Lenkungsausschuss, einer beratenden Funktion angesiedelt bei der Projektleitung bis hin zur aktiven Mitarbeit in den einzelnen Projektgruppen gehen. Unabhängig von der genauen Position im Projekt und von dem Umfang der personenbezogenen Daten im BW empfiehlt die Arbeitsgruppe Datenschutz, dass der Datenschutzbeauftragte Mitglied des SAP BW Projekten sein sollte. Denn selbst in dem Fall, in dem am Ende das Projekt entscheidet, dass keine personenbezogenen Daten im BW gespeichert werden sollen, gibt es erfahrungsgemäß erheblichen Beratungsbedarf über die Frage, wie personenbezogene Daten der Quellsysteme herausgehalten, also anonymisiert, pseudonymisiert oder aggregiert werden und eine Wiederherstellung des Personenbezugs verhindert werden kann.

Um dies beurteilen zu können, brauchen die Datenschutzverantwortlichen gewisse Grundkenntnisse über die von SAP zur Verfügung gestellten Techniken und deren Einstellungsmöglichkeiten. Dies kann durch Lektüre der Dokumentation (siehe <http://help.sap.com>), des Sicherheitsleitfadens, des allgemeinen *Leitfadens Datenschutz für SAP R/3* und unter Umständen auch durch den Besuch gewisser Schulungen bei der SAP AG oder anderen Institutionen erreicht werden.

2.2.1.2 Business Blueprint

Im Rahmen der Phase des *Business Blueprint* gilt es das Datenmodell zu konzipieren, die Einzelheiten der Datenübernahme von den Quellsystemen in das SAP BW festzulegen, Aus-

wertungen und Auswertungsmöglichkeiten zu planen, Benutzerrollen und Berechtigungen zu entwickeln, sowie einen Plan für die Benutzerschulung und Dokumentation zu erstellen.

Im Rahmen des Datenmodells und der Datenübernahme sind einerseits die oben schon einmal genannten Grundentscheidungen zu treffen: Kommen personenbezogene Daten in das BW? Wenn ja, können diese ggf. anonymisiert, aggregiert oder pseudonymisiert werden? Wenn ja, an welcher Stelle – im Quellsystem oder im Zielsystem, im Eingangsbereich oder bei der Bildung der InfoCubes? Entscheidet sich das Projekt dafür, personenbezogene Daten im BW abzulegen, dann sind gewisse Folgeaktivitäten zur Erfüllung der datenschutzrechtlichen Anforderungen zwingend zu diskutieren, wie etwa:

- Gibt es für die vorgesehene Verarbeitung der personenbezogenen Daten im BW eine Rechtsgrundlage?
- Wenn das BW in einer rechtlich anderen Gesellschaft – etwa der Konzernmutter - betrieben wird, ist zu klären, welche Rechtsgrundlagen zur Übermittlung der Daten bestehen und für welche Zwecke der Empfänger die Daten verarbeiten darf; Welche Einschränkungen bei den Auswertungen und bei der Nutzung von Auswertungswerkzeugen ergeben sich ggf. aus den Rechtsgrundlagen?
- gibt es die Möglichkeit mit anonymisierten Daten oder Pseudonymen zu arbeiten und trotzdem die Datensätze zuzuordnen (etwa durch verschlüsselt abgelegte Ordnungsschlüssel in der Staging Area, durch Bildung von Info Cubes mit aggregierten Daten, etc.),
- Welche Auswertungsmöglichkeiten und –formen sind im Rahmen der Zweckbindung der Datenverarbeitung zulässig?
- in welcher Form sind die zu liefernden Übersichten zu führen (siehe dazu auch den Abschnitt 2.3 weiter unten),
- welche technisch-organisatorischen Maßnahmen – insbesondere im Rahmen der Zugriffsrechte - sind erforderlich, etc.

Weiter bedarf es bei der Planung der Auswertungen und Auswertungsmöglichkeiten gewisser rechtlicher Überlegungen zur Prüfung der Rechtsgrundlagen für die Speicherung, Verarbeitung und Löschung, sowie ggf. zur Übermittlung der Daten, wenn der Zugriff auf die Daten des BW auch von Außenstehenden – etwa Konzerncontrollern - erlaubt sein soll. Auch hier ist jeweils zu prüfen, ob fehlende Rechtsgrundlagen durch neu zu schaffende Rechtsgrundlagen in Verträgen und Vereinbarungen ersetzt werden. Besondere Beachtung verdienen bei grenzüberschreitendem Datenzugriff die Vorschriften des Kapitels IV der EU Richtlinie 95/46/EG Artikel 25f. und deren Umsetzung in nationales Recht.

Schließlich sind die Anforderungen an Benutzerrollen und die zugehörigen Berechtigungen zusammenzustellen. Im Rahmen des Schrittes der Schulung und Dokumentation sind die jeweiligen datenschutzrechtlichen Kenntnisse der zukünftigen Nutzer zu erheben und der damit im Zusammenhang bestehende Informationsbedarf festzuhalten.

2.2.1.3 Realisierungsphase

In der *Realisierungsphase* sind die konzipierten Anforderungen der vorherigen Phasen durch Einstellungen am System und ggf. weitere Programmierung umzusetzen. Gegebenenfalls erforderliche Änderungen sind durchzuführen und zu testen. Dem Datenschutzverantwortlichen kommt dabei die Aufgabe zu, die anforderungsgerechte Umsetzung zu begleiten und das Pro-

jekt entsprechend zu beraten. Insbesondere sind in dieser Phase folgende Aktivitäten für den Datenschutz von Belang:

- die organisatorischen Änderungen (z.B. Fragen von Zuständigkeiten, etc.)
- die Planung der Schulungs- und Dokumentationsaktivitäten (inkl. der Frage, ist eine breitere Unterweisung der zukünftigen Nutzer in Belangen des Datenschutzes erforderlich? Wenn ja mit welchen Inhalten und in welcher Form),
- die Entwicklung der Benutzerrollen und die Einstellung der Berechtigungen (technisch—organisatorische Maßnahmen im Sinne des Artikel 17 der EU Richtlinie, bzw. entsprechend der jeweiligen national geltenden Vorschriften wie etwa §9 BDSG), sowie
- die Entwicklung des Vergabeverfahrens für neue Berechtigungen und Benutzer (ebenefalls im Rahmen der oben zitierten technisch-organisatorischen Maßnahmen);
- Customizing, insbesondere die Maskengestaltung (entsprechend Artikel 7 und 8 der EU Richtlinie, damit auch nur derjenige genau die Daten sieht, die er im Rahmen seiner rechtlichen Aufgabenerfüllung bearbeiten muss) ;
- die Entwicklung und Tests der Auswertungen und Workflows;
- die Konfiguration des Datenextraktes aus den Quellsystemen (zur Umsetzung des Prinzips der Datensparsamkeit und Datenvermeidung insbesondere dann, wenn das Quellsystem und das BW unterschiedlichen Rechtskreisen zuzuordnen sind, dass heißt eine Datenübermittlung im rechtlichen Sinne stattfindet);
- Konzeption der Datenflüsse;
- die Archivierung (insbesondere zur Prüfung der Aufbewahrungs- und Lösungsfristen) und
- Test und Abnahme der Einstellungen;

2.2.1.4 Produktionsvorbereitung, bzw. Final Preparation

In der Produktionsvorbereitung werden unter Datenschutzgesichtspunkten insbesondere das Überspielen und Testen der Funktionen mit echten Daten vorgenommen, die Schulung der Endanwender durchgeführt und die Wirksamkeit der technisch-organisatorischen Sicherheitsmechanismen überprüft. Vergleiche zu letzterem insbesondere die SAP Empfehlungen im Sicherheitsleitfaden und speziell im Rahmen der Qualitätssicherung die Checklisten im Teil 3 des Sicherheitsleitfadens.

2.2.1.5 Go Live and Support

Im Rahmen der Aufnahme des Produktivbetriebs sind auch aus Datenschutzsicht Qualitätssicherungsmaßnahmen vorzusehen, die in einem kontinuierlichen Prozess ständig den Zustand der Datenschutzmaßnahmen prüfen und verbessern helfen. Erfahrungsgemäß sind bei Projekten dieser Größenordnung in der Einführungsphase und auch bei Releasewechseln Themen übersehen worden, die erst im Rahmen späterer Überprüfungen entdeckt und verbessert werden können.

2.2.1.6 Empfehlung zur Vorgehensweise

Nehmen Sie sich den jeweils aktuellen ASAP/Solution Manager Einführungsleitfaden vor. Identifizieren Sie im Ablaufplan die aus Ihrer Sicht relevanten Schritte und Beschleuniger (beide sind Teil der Unterlagen). Gehen sie die einschlägigen Dokumente mit den Projektverantwortlichen durch, besprechen Sie die datenschutzrechtlich relevanten Anforderungen und stimmen Sie die Projektergebnisse im Laufe des Projektes ab. Lassen Sie sich zu diesem Zwecke laufend den aktuellen Projektstand berichten und greifen Sie zu den einschlägigen Themen in die Diskussion ein.

2.2.2 Business Content

Business Content sind vorkonfigurierte, auf konsistenten Metadaten basierende rollen- und aufgabenbezogene Informationsmodelle im SAP Business Information Warehouse. Der Unternehmen alle Objekte für den schnellen Aufbau ihres Berichtswesens zur Verfügung stellt – von der Datenextraktion bis hin zu Rollen, die den Mitarbeitern im Unternehmen alle Informationen zur Verfügung stellen, die sie zur Erfüllung ihrer Aufgaben benötigen. Der vordefinierte Business Content hilft dabei, die Implementierungszeit drastisch zu senken und zwar unabhängig davon, ob dieser Content, wie von SAP festgelegt, integriert wird oder als Ausgangspunkt dient, um kundenspezifische Modelle zu erstellen.

Diese Informationsmodelle umfassen im wesentlichen Rollen, Arbeitsmappen, Queries, InfoSources, InfoCubes, ODS-Objekte, Kennzahlen, Merkmale, Fortschreibungsregeln sowie Extraktoren für SAP R/3, mySAP.com Business Applications und für weitere ausgewählte Anwendungen.

Business Content kann:

- ohne Anpassung verwendet werden
- angepasst, d.h. verfeinert oder vergrößert werden
- als Vorlage oder Beispiel für selbsterstellten Business Content dienen

Darüber hinaus wird mit dem SAP Business Information Warehouse Demo Content zur Verfügung gestellt, der Beispieldaten umfasst und als Anschauungsmaterial verwendet werden kann.

Unter dem Sammelbegriff "Business Content" liefert das SAP Business Information Warehouse vorkonfigurierte Objekte. Diese Objekte beschleunigen die Einführung des SAP Business Information Warehouse, da sie fertige Lösungen für den Bedarf an betriebswirtschaftlichen Informationen liefern.

Der Business Content umfasst:

- R/3 Extraktor-Programme
- DataSources
- Prozessketten
- InfoObjects
- InfoSources
- Datenziele (InfoCubes und ODS-Objekte)

- Variablen
- Data Mining-Modelle
- Queries
- Arbeitsmappen
- Crystal Reports
- Web Templates
- Rollen

Das Vorgehen der Einführung mittels Analyse und Abänderung der Vorlagen des Business Content umfasst grob folgende datenschutzrelevante Schritte:

- Projektstart mit Definition der Projektziele und Projektschritte
- Projektplanung
- Bildung der Projektgruppen
- Schulung der Projektmitglieder
- Einrichtung des Zugangs zu einem System mit Business Content
- Erstellung eines Sollkonzeptes für die Änderungen an den verschiedenen Objekten, insbesondere
 - o Änderung der Eingangsdaten (DataSources)
 - o Änderung des Datenmodells (InfoObjects, InfoSources, InfoCubes und ODS Objekte)
 - o Änderungen der Sichten (Bildung von MultiCubes, Queries)
 - o Änderung der Berechtigungsprüfungen
 - o Änderung der Darstellungen der Auswertungen für den Endbenutzer
- Änderung hinsichtlich der zur Verfügung gestellten Werkzeuge
- Erstellung und Test eines Berechtigungskonzeptes
- Implementierung der Veränderungen
- Test der Veränderungen
- Produktivschaltung

Ein formalisiertes Vorgehen – wie bei der Nutzung des Solution Manager – gibt es bei der Abänderung des Business Content nicht. Das konkrete Vorgehen in den Projekten hängt dabei stark von dem Erfüllungsgrad der betrieblichen Anforderungen durch den Business Content ab.

Wenn nun in einem Unternehmen ein Projekt zur Einführung des BW unter Nutzung des BC „gestartet“ wird, ist der betriebliche/behördliche Datenschutzbeauftragte (und in vielen Fällen auch die Arbeitnehmervertretung aufgrund von Mitbestimmungstatbeständen z.B. § 87. Abs.1 Satz 6) frühzeitig mit einzubeziehen.

Weiterführende Ansatzpunkte, wo personenbezogene Daten im Business Content verarbeitet werden, sind im Zusammenhang mit den vorbereiteten Auswertungen im Kapitel 2.7 zu finden.

2.3 Übersichten

Für die Wahrnehmung seiner Aufgaben erhält der DSB die nach den §§ 4e und 4g Abs. 2 BDSG geforderten Unterlagen (s. *Leitfaden Datenschutz für SAP R/3*, Kap. 2.3).

Die EU-Datenschutz-Richtlinie definiert in Artikel 19 - **Inhalt der Meldung** - den Mindestumfang der Angaben:

(1) Die Mitgliedstaaten legen fest, welche Angaben die Meldung zu enthalten hat. Hierzu gehört zumindest folgendes:

b) die Zweckbestimmung(en) der Verarbeitung;

c) eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien;

d) die Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;

e) eine geplante Datenübermittlung in Drittländer;

f) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 17 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

(2) Die Mitgliedstaaten legen die Verfahren fest, nach denen Änderungen der in Absatz 1 genannten Angaben der Kontrollstelle zu melden sind.

Zweck der Übersichten ist es, dem Beauftragten für Datenschutz die Wahrnehmung seiner Aufgabe

- zur Prüfung der Zulässigkeit der Verarbeitung personenbezogener Daten
- zur Vorabkontrolle und
- zur Unterrichtung und Schulung der Benutzer
- zur Benachrichtigung und Auskunft an die Betroffenen

zu ermöglichen, der Aufsichtsbehörde die Kontrolle der Durchführung von Datenschutzvorschriften zu erlauben und außerdem die Transparenz der Datenverarbeitung für Jedermann zu schaffen.

Im *Leitfaden Datenschutz für SAP R/3*, Release 4.6, wird in den Abschnitten 2.3 (Führen von Übersichten) ausführlich auf die Form der Dokumentation, das öffentliche Melderegister und das betriebsinterne Verzeichnisse im Zusammenhang mit dem SAP R/3-System eingegangen. Auf diese Ausführungen wird ausdrücklich verwiesen.

SAP BW-Systeme werden i.d.R. zusätzlich zu R/3-Systemen betrieben, sodass die Vorstellung naheliegender ist, einfach auf die dort gefertigten Übersichten zu verweisen. Dies reicht aber in keinem Fall aus. Denn selbst wenn eine 1-1-Übernahme (Spiegelung) einer operativen SAP R/3-Anwendung erfolgt, bedarf es zumindest besonderer technisch-organisatorischer Anstrengungen, um etwa die Berechtigungsstrukturen für Auswertungen durch firmenspezifische Berechtigungsobjekte abzubilden (vgl. hierzu die Ausführungen in den Abschnitten 2.7 und 2.8).

In der Regel **sind für das SAP BW Ergänzungen der Übersichten erforderlich**, weil

- die Verarbeitungszwecke im Sinne des § 4e Ziffer 4 für das BW oft nicht mit den Verarbeitungszwecken der Quellsysteme identisch sind und von den Rechtsgrundlagen auch nicht mehr gedeckt sind,
- die Empfänger oder Kategorien von Empfängern häufig über die der Quellsysteme hinausgehen (Beispiel: firmenübergreifende BWs),
- die Aufbewahrungsfristen und Regelfristen der Löschung sich in einem BW nach anderen Grundsätzen bestimmen, als in den Quellsystemen,
- auch die Übermittlung in Drittländer (in firmenübergreifenden BWs) anders gehandhabt werden kann, als in den Quellsystemen,
- das BW auf jeden Fall eigenständige technisch-organisatorische Maßnahmen zur Sicherung der dort gespeicherten und ausgewerteten Daten erfordert (z.B. firmenspezifische Berechtigungsobjekte für das Reporting).

Die **Form der Übersichten für ein SAP BW** mit personenbezogenen Daten kann der Form der sonst auch geforderten Verfahrensverzeichnissen entsprechen (vgl. insoweit den *Leitfaden Datenschutz für SAP R/3*, Kapitel 2.3.9). Es ist aber zu bedenken, dass alle Verarbeitungszwecke vor dem Einsatz neuer Verarbeitungen aufzuführen sind. Bei nachträglich definierten zusätzlichen Zwecken, die über die „alten“ Verarbeitungszwecke hinausgehen, sind die Verzeichnisse vor der Verarbeitung fortzuschreiben. Der Datenschutzbeauftragte muss vor dem Einsatz einer neuen Verarbeitung personenbezogener Daten (auf der Basis des fortgeschriebenen Verfahrensverzeichnisses) die Chance haben, das Verfahren zu begutachten.

Zur Dokumentation der **Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung** siehe die Bemerkungen zu 2.3.2 im *Leitfaden Datenschutz für SAP R/3*.

Die **Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien** kann im SAP BW durch Rückgriff auf die Daten in elementaren Bausteinen des BW - die InfoObjects bzw. die InfoSources, mit denen der Datentransport aus den Quellsystemen ermöglicht wird - erfolgen.

Zusätzlich liefert das BW Metadata Repository weitere Informationen über die Datenstrukturen. (vgl. hierzu Kap. 2.1).

Außerdem kann zur Beschreibung auch die BW Statistik verwendet werden. Rufen Sie hierzu die Administrator Workbench (Transaktion RSA1) auf und wählen Sie dort den Bereich *Modellierung*. Wählen Sie den InfoProvider-Baum. Dort finden Sie unter der InfoArea *Technischer Content* die InfoArea *BW Statistik*, unter der alle InfoProvider zur BW Statistik zu finden sind.

Hierbei handelt es sich um ein Analysewerkzeug, das im technischen Content des BW enthalten ist und z.B. einen Überblick über die Nutzung von InfoObjects, InfoSources, Quellsystemen und Queries ermöglicht (-> technische Beschreibung in Abschnitt 2.4). Folgende Fragestellungen können mit der BW Statistik z.B. beantwortet werden:

- Welche InfoCubes, InfoSources, Queries, Aggregate werden im System genutzt?

Beim Vergleich der SAP Auslieferungsversion (D-Version) mit der aktiven Version (A-Version) kann man überprüfen, welche Objekte benutzt werden. Um mit Objekten arbeiten zu können, müssen diese in die aktive Version (A-Version) überführt werden.

- Welche Daten werden von wo nach wo transportiert?

- Welche Daten in InfoCubes, InfoObjects, InfoSources, Quellsysteme, Queries, Aggregate werden aktuell im System genutzt?

Mit Hilfe des technischen Contents (BW Statistik) kann man beantworten, welche Abteilungen oder Benutzer das BW über eine bestimmte Zeitspanne hinweg (z.B. im letzten Quartal; im letzten Jahr) verwendet haben.

Infosources und Quellsystem überprüft man am besten mit der Transaktion RSA1.

- Welche Datenbestände werden bewegt?

Diese Informationen werden beim Ausführen von InfoPackages erzeugt.

- Welcher Benutzer arbeitet gerade im System?

Mit der Transaktion SM04 bekommt man wie im R/3 eine gegenwärtige Benutzerliste angezeigt

- Datenausgang

Soll ein schon existierendes Business Information Warehouse als Quellsystem definiert werden, wird hierfür die Funktionalität des Data Mart Interfaces verwendet.

Möchten Sie ein schon existierendes Business Information Warehouse als Quellsystem definieren, so greifen Sie auf die Funktionalität des Data Mart Interfaces zu. Das Data Mart Interface kann zwischen zwei BW-Systemen oder zwischen einem APO-System (Advanced Planner and Optimizer) und einem BW-System eingesetzt werden.

Der Open Hub Service ermöglicht es, Daten aus einem SAP BW System in nicht-SAP Data Marts und anderen Anwendungen zu verteilen. Damit wird die kontrollierte Verteilung über mehrere Systeme hinweg gewährleistet.

Die **Empfänger oder Kategorien von Empfängern**, denen personenbezogene Daten im Rahmen des SAP BW mitgeteilt werden können, lassen sich ggf. aus den Kommunikationsstrukturen der InfoSources bzw. über das Berechtigungskonzept beschreiben (vgl. hierzu Kap. 2.8).

Zugriffsberechtigte Personen oder Personengruppen

Mit dem Infosystem Berechtigungen (Transaktionen SUIM) stehen im BW dieselben Auswertungen über Benutzer und Berechtigungen wie im R/3-System zur Verfügung.

Beispiel einer Übersicht inklusive SAP BW

Bei nachfolgendem Beispiel wird auf den *Leitfaden Datenschutz für SAP R/3* (Kap. 2.3.9) Bezug genommen.

Öffentlicher Teil für Jedermann

Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung

mySAP BW: Ermittlung und zur Verfügungstellung von Kennziffern auf der Basis von aggregierten Daten für die Personaladministration, für die dezentrale Organisationssteuerung, Personalbeschaffung, Personalbetreuung (Vergütung, Arbeitgeberleistungen, Altersvorsorge), strategische Personalplanung und Personalkostenplanung

Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien

Personen: Mitarbeiter, Bewerber, Kunden, Lieferanten, Versicherungsnehmer

Daten: Mitarbeiter-, Bewerber-, Kunden-, Lieferanten- bzw. Versicherungsnehmer-Daten aus mySAP HR, mySAP FI und mySAP CRM

Besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Art. 8 EU-RL), zum Beispiel: betriebliche Gesundheitsschutz- bzw. Arbeitsschutzdaten aus Unfallmeldungen,

Empfänger oder Kategorien von Empfängern

Auftragsdatenverarbeiter, konzernverbundene Unternehmen, insbesondere Holding

Regelfristen für die Löschung der Daten

Periodische Löschung nach Ablauf einer z.B. 3-jährigen Aufbewahrungsfrist;

Verdichtung zu aggregierten Datensätzen jeweils im dritten Jahr

Geplante Datenübermittlung in Drittstaaten

Beispiel: Konzernmutter in Japan; Vertriebsfirmen in Mittelamerika, USA und Australien

Nichtöffentlicher Teil

Allgemeine Beschreibung zur Beurteilung der Angemessenheit der Schutzmaßnahmen nach § 9 BDSG

- Vorlage eines gesonderten Sicherheitskonzepts
- Vorgesehene Protokollauswertungen: Security Audit Log, Syslog
- Systemumgebung: Systemsoftware (Betriebssystem, DB, Netzwerk), Anwendungssoftware (mySAP BW)

Technisch-organisatorische Maßnahmen nach § 9 BDSG:

Kontrolle: bDSB

Zutritt: Pförtner, Schlüssel

Zugang: PC-Sperre, Kennwortregeln

Zugriff: Berechtigungskonzept und Schutz der Programme vor Veränderung durch Anwender

Weitergabe: siehe Zugriffsberechtigungen

Eingabe: Änderungsbelege in den Quellsystemen; zum Teil durch BW- Ladeprotokolle

Auftrag: vertragliche Regelungen und Stichproben durch Revision und DSB

Verfügbarkeit: DB-Recovery, Sicherungskopien außer Haus

Trennung: Abschottung durch Rollen/Berechtigungen; kein Download zugelassen

Aufgaben und Berechtigungen des DSB

Um die datenschutzgerechte Einrichtung eines SAP BW zu beurteilen oder die erforderlichen Prüfungshandlungen vorzunehmen, ist eine ausreichende Ausbildung des Datenschutzbeauftragten in der Nutzung der relevanten SAP BW-Funktionen notwendig. Außerdem sollte der DSB über die erforderlichen Zugriffsberechtigungen im SAP BW verfügen.

Auf Empfehlung der AG Datenschutz wird SAP eine Standardrolle für den Datenschutzbeauftragten, z.B. SAP_Auditor_BW, entwickeln. Diese Rolle muss an die betrieblichen Anforderungen angepasst werden.

Wir empfehlen den Anwenderfirmen bis zur Auslieferung dem Datenschutzbeauftragten die Rolle

Z_AUDITOR_BW (Namensvorschlag)

(mit Leseberechtigung) zu erteilen, mit der u.a. folgende Funktionen zugreifbar sind:

- BW Statistik MultiProvider bzw. -Queries
- Basis Anzeigeprofil S_A.SHOW (zzgl. der Berechtigung zum Anzeigen von Änderungsbelegen der Berechtigungsverwaltung und abzüglich der Berechtigung zur Anzeige von Anwendungsdaten⁴)
- Administrator Workbench (RSA1): Die Berechtigung ist in den Berechtigungsobjekten S_RS_* auf „Anzeigen“ und Teilobjekt „Definition“ zu beschränken.
- Monitor Administrator Workbench (RSMO)
- Query Monitor RSRT

Die letzten drei Transaktionen haben ggf. Schreibberechtigung. In diesem Fall ist die Hilfe des Administrators notwendig.

Techniken zur Erstellung von Übersichten für SAP BW

BW Metadata Repository:

Mit dem HTML-basierten BW Metadata Repository können Sie zentral auf Informationen zu den Metadaten des BW, wie etwa die wichtigsten Eigenschaften der Objekte und die Verknüpfungen mit anderen Objekten, zugreifen. Sie können dabei Metadaten suchen, Metadaten austauschen, HTML-Seiten exportieren und Grafikdarstellungen der Objekte anzeigen.

Funktionsumfang:

Im Metadata Repository können sich sowohl aktive Objekte im System (Aktivierte Objekte) als auch SAP-Auslieferungsobjekte im System (Business Content) anzeigen lassen. Im rechten Fenster werden die im jeweiligen System vorhandenen Objekttypen aufgeführt. Über Hyperlinks erhalten Sie zu jedem Objekttyp eine Liste aller Objekte dieses Objekttyps. Von dieser Objektliste können Sie direkt zu den einzelnen Objektinformationen navigieren.

Suche im Metadata Repository:

⁴ Im Berechtigungsobjekt S_TABU_DIS ist die Anzeige auf Customizing- und Systemtabellen zu beschränken.

Dabei werden die technischen Namen, die Kurz- und Langtexte und die ausgelieferte SAP-Dokumentation der im Metadata Repository vorhandenen Objekte durchsucht. HTML-Export:

Es können sowohl aktive Objekte als auch SAP-Auslieferungsobjekte komplett als HTML-Seiten exportiert werden. Diese können dem Datenschutzbeauftragten zur Verfügung gestellt werden.

Grafiken:

Metadaten können durch XML-basierte Vektorgrafik-Formate für Dokumente und das Internet als VML-Graphiken und SVG-Graphiken angezeigt werden.

2.4 Auftragsdatenverarbeitung

Bei der Einschaltung eines Dienstleisters beim Betrieb des BW sind die Voraussetzungen der Auftragsdatenverarbeitung bzw. Funktionsübertragung zu beachten. Zu den diesbezüglichen Grundsätzen wird auf Kapitel 5 im *Leitfaden Datenschutz für SAP R/3* verwiesen.

Bei der Ausgestaltung des Dienstleistungsverhältnisses sind folgende Fälle zu beachten:

Fall 1:

Das Gesamtsystem (operatives System und BW) wird durch einen Dienstleister betrieben. Hier ist der Dienstleistungsvertrag nur um die Leistungsfelder des BW zu ergänzen.

Fall 2:

Nicht das Gesamtsystem, sondern nur eine oder mehrere Komponenten (operatives System, Basis des BW oder InfoCubes) werden durch einen Dienstleister betrieben.

Bei Einschaltung eines Dienstleisters wird regelmäßig für den von ihm ausgeführten Service eine Auftragsdatenverarbeitung im Sinne des Datenschutzrechts vorliegen, insoweit sind – unabhängig von der grundsätzlichen Zulässigkeitsprüfung (s. Kap. 1) – die Voraussetzungen von § 11 BDSG zu beachten, s. Kapitel 5 im *Leitfaden Datenschutz für SAP R/3*.

Sonderfall Funktionsübertragung:

Soll der BW-Betreiber selbständig mit den Daten umgehen können (zum Beispiel bei unternehmensübergreifenden Auswertungen der Konzernmutter), setzt dies in der Regel eine vorherige Datenübermittlung voraus. Insoweit ist eine Auftragsdatenverarbeitung nicht gegeben, hier sind die Bestimmungen zur Datenübermittlung anzuwenden, s. Kapitel 5 im *Leitfaden Datenschutz für SAP R/3*.

Sonderfall Drittland:

Gelangen personenbezogene Daten im Zusammenhang mit dem Betrieb eines BW in ein Land außerhalb der EU oder des EWR sind neben den Zulässigkeitsvoraussetzungen für den Betrieb des BW (s. Kapitel 1) zusätzlich die Anforderungen an den so genannten Drittlandstransfer im Hinblick auf ein angemessenes Datenschutzniveau zu beachten (§§ 4b, 4c BDSG, Art. 25, 26 EU-RL, siehe Kapitel 2.3.6 und 5.2.9 im *Leitfaden Datenschutz für SAP R/3*).

Um den Zugriff aus Drittländern zu erlauben, wäre ggf. ein getrenntes BW-System denkbar, an das entsprechend anonymisierte oder pseudonymisierte Daten übermittelt werden.

2.5 Datenübernahme (Anonymisierung, Pseudonymisierung)

Durch das Zusammenführen von Daten aus den unterschiedlichsten Systemen verfolgt man das Ziel, eine einheitliche und konsistente Sicht auf Kunden, Geschäftsabläufe und andere Aspekte des Unternehmensgeschehens zu erhalten. Diese Zusammenführung ist wegen dem datenschutzrechtlich unabdingbaren Zweckbindungsgebot meist problematisch. Personenbezogene Daten sind für festgelegte eindeutige und rechtmäßige Zwecke zu erheben. Die Daten dürfen nicht mit einer mit dieser Zweckbestimmung nicht zu vereinbarende Weise weiterverarbeitet werden.⁵

Als Zulassungskriterium bleibt oft nur die Einwilligung der Betroffenen oder die Anonymisierung bzw. Pseudonymisierung. Liegt eine Anonymisierung aller personenbezogenen Daten vor, d.h. es kann nicht mehr auf die Einzelperson rückgeschlossen werden, gelten nicht mehr die strengen Bestimmungen des BDSG.

Ein Data Warehouse ist relativ statisch und in der Regel für die Abfrage großer Mengen historischer Daten ausgelegt. Es wird im Gegensatz zur operativen Entscheidungsunterstützung bei der strategischen Entscheidungsfindung eingesetzt.

Man sollte sich deshalb zunutze machen, dass in vielen Fällen der Zugriff auf personenbezogene Daten im BW-System nicht benötigt wird, um zu globalen Erkenntnissen zu gelangen. Zu Projektbeginn darf nicht die Frage stehen, welche Daten man überhaupt aus den operativen Systemen extrahieren kann, sondern welche Informationen die Nutzer benötigen, um die Herausforderungen des Geschäftsalltags zu meistern. So benötigt man z.B. konzernweit bei der Personalplanung aggregierte Informationen über Personalbestand, Personalbewegungen oder Mitarbeiterstruktur, persönliche Details von einzelnen Mitarbeitern wie Alter, Geschlecht, Nationalität, Skills oder Ausbildung verbleiben jedoch in den BW-Zubringersystemen und können bei einer folgenden Detailanalyse dort von den Berechtigten dieser Systeme eingesehen werden.

Oft genügen also Übersichten auf Kostenstellenebene ohne einen *Drill Down* auf die Einzelperson.

Hier gibt sich für den Datenschutzbeauftragten die Chance, den Forderungen nach Datenvermeidung und Datensparsamkeit nachzukommen. Er sollte die Chance nutzen, sich schon bei der Projektplanung in das Projekt einzubringen und bereits bei der Datenübernahme die Möglichkeiten zur Anonymisierung und Pseudonymisierung zu erörtern. Zusammen mit der Arbeitnehmersvertretung kann geprüft werden, ob ein Personenbezug notwendig ist. Die Gefahr einer potentiellen Leistungsbeurteilung kann auf diesem Wege ebenfalls eingedämmt werden.

2.5.1 Anonymisierung oder Pseudonymisierung bei Übernahme

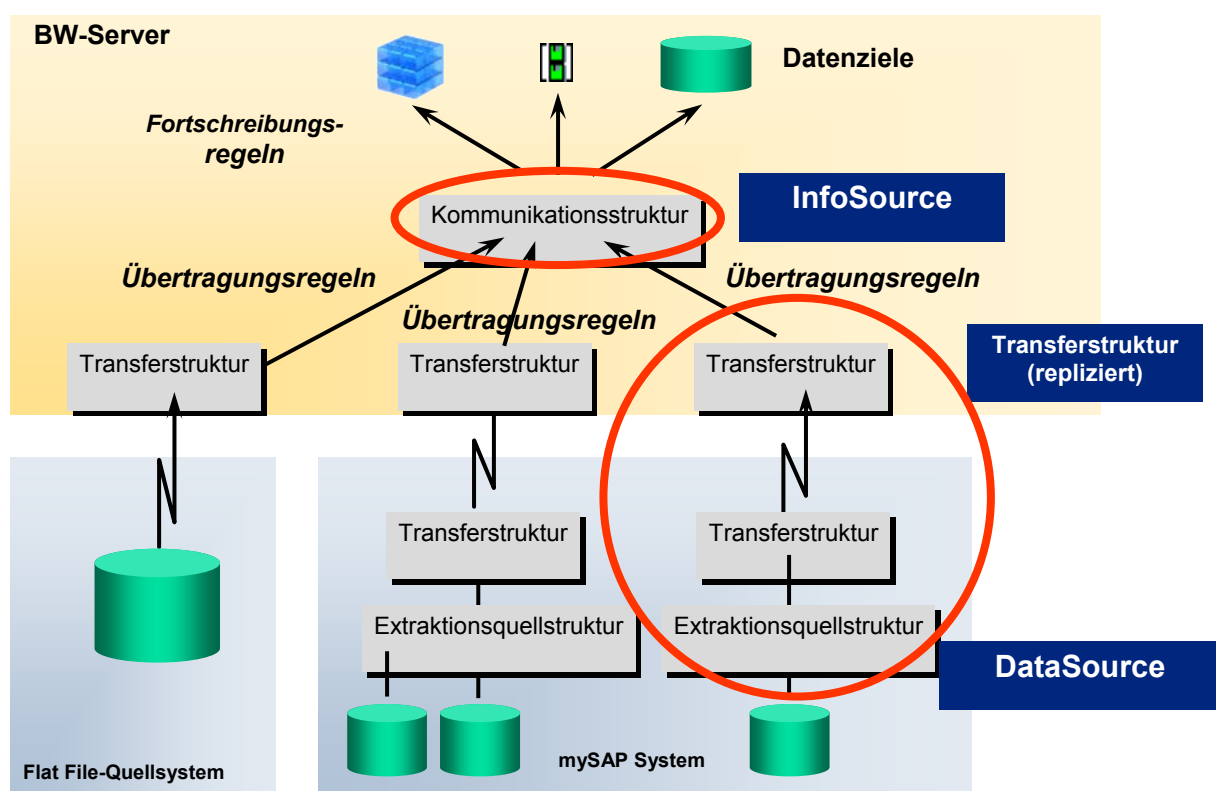
Aus Gründen der Datensparsamkeit dürfen nur die unbedingt benötigten Daten aus den Quellsystemen kopiert werden. Entsprechend der Datenschutzgrundsätze müssen die Daten sachlich richtig und auf dem neuesten Stand sein. Zunächst ist zu prüfen, ob es eine Möglichkeit gibt, schon im Quellsystem bzw. auf einer Kopie eine Anonymisierung bestimmter Felder

⁵ Art 6 EU-Richtlinie

durchzuführen. Entsprechende Programme werden auf dem Markt auch für HR angeboten⁶. Die Aussagekraft der Daten im BW muss davon unberührt bleiben.

Bei der Übernahme muss grundsätzlich geprüft werden, welche personenbezogenen Daten in das BW-System transportiert werden müssen. Es ist durchaus möglich, dass man mehr Daten vom Quellsystem extrahiert, als man für die Auswertung benötigt. In den ODS Objekten und den InfoCubes können auf diese Art und Weise Daten schlummern, die zwar nie vom Endbenutzer angezeigt werden, aber zumindest zum Aufbau der Informationseinheiten benötigt wurden. Hier ist zu beachten, dass diese Daten eventuell privilegierten Benutzern wie der Administration zugänglich sind oder auch das Ziel von Angriffen, wenn das SAP BW nicht den entsprechend hohen Sicherheitsstand hat wie z.B. das originale Personal- oder die Kundensystem.

Welche Möglichkeiten bietet uns hier das SAP BW?



SAP-Technik: Extrahieren, Transformieren und Laden

Um aussagekräftig zu sein, müssen die übernommenen Daten integriert, standardisiert und konsistent sein. Dies erfolgt über den ETL-Prozess (Extrahieren, Transformieren und Laden).

ETL ist ein anspruchsvoller Bestandteil von Data Warehousing. Nicht nur die richtigen Datenquellen sind zu identifizieren, sondern auch der Wert und die Zuverlässigkeit der Daten

⁶ Firmen wie BKC in Münster, Inside GmbH in Oldenburg (<http://www.inside-net.de/>), PECASO in Heidelberg (www.pecaso.com -> Clone&Test) oder SQS in Köln (http://www.sqs.de/solutions/solu_saptest.htm -> Testsuite für SAP R/3) bieten entsprechende Programme an.

müssen beurteilt werden. An dieser Stelle sollte der Datenschutzbeauftragte auch die Zulässigkeit der Daten prüfen.

Extrahieren

Die Datenextraktion erfolgt entweder auf der Anwendungsebene oder auf der Datenbank- oder Dateiebene (der „technischen Ebene“).

Auf der Anwendungsebene werden die Daten in Form von Geschäftsobjekten (Business Objects) extrahiert. Meist wird ein Geschäftsobjekt in mehreren Tabellen dargestellt. Die Beziehung zwischen den Tabellen wird von der Anwendungslogik definiert.

Insbesondere SAP-Anwendungen können nahtlos ins SAP BW integriert werden. Über den Datenextraktor können spezielle Extraktoren für spezielle Objekte innerhalb des Quellsystems (z. B. für „Bestellung“ in mySAP CRM) verwendet werden. Mit Extraktoren können auch immer wieder Deltas aus den Quellsystemen übernommen werden, um auf Komplettübertragungen verzichten zu können. Der Benutzer legt hier selbst fest, in welchem Rhythmus Daten aktualisiert werden sollen.

Die Staging BAPI (Business Application Programming Interface) erlaubt die Übernahme aus Nicht-SAP-Quellen. Dies ist besonders für Unternehmen wichtig, die intern entwickelte Datenextraktionsprogrammen vorziehen.

Die Extraktion auf der Datenbank- und Dateiebene setzt den Abruf der Daten und der entsprechenden Metadaten direkt aus diesen unterschiedlichen Tabellen voraus. Diese Form der Extraktion ist geeignet, wenn sich die Daten in „flachen“ Dateien befinden, wenn sie über XML gesendet werden oder in Datenbanken von Alt-Anwendungen gespeichert sind.

SAP BW bietet umfangreiche ETL-Funktionen, die eine Datenextraktion sowohl auf Anwendungs- als auch auf Datenbank und Dateiebene ermöglichen.

Die Quelldaten werden physisch unverändert im PSA-Objekt (Persistent-Staging-Area-Objekt), einer transparenten Datenbanktabelle, gespeichert. Die PSA ist der Eingangsspeicher der Daten im Informationsmodell von SAP BW. Eine PSA wird für jede DataSource und jedes Quellsystem erstellt.

Transformieren

Der nächste logische Schritt ist die Verschiebung von der DataSource in die InfoSource, die InfoObjects enthält, die aus Sicht des Unternehmens logisch zusammengehören. Über die angewendeten Transformationsregeln werden hierbei die Daten bereinigt und in Informationen verwandelt.

SAP BW bietet eine reichhaltige Bibliothek mit Transformationsregeln, mit denen den Daten bei Datum-/Zeit-Konvertierungen, Zeichenfolgenoperationen, Aggregationen usw. die jeweilige Geschäftslogik zugeordnet wird. Diese Transferregeln können einfach über die Verwendung von Formeln mithilfe einer Transformation Toolbox eingebunden werden, wenn man auf eigene Codierung verzichten will. Im Zuordnungsprozess wird also genau festgelegt, welche Daten aus der DataSource in die InfoSource transferiert werden.

Realisierung

Im Regelwerk der Übernahme ist auch eine systematische Anonymisierung oder Pseudonymisierung möglich, so können z.B. Kundenname, Ort und Straße beliebig überschreiben oder ersetzt werden.

Beispiel:

Das Datenangebot eines Quellsystems wird durch DataSources in betriebswirtschaftliche abgeschlossene Bereiche untergliedert. DataSources stellen quellsystemabhängige DataSource-Typen dar, die zur Übertragung von Stamm- und Bewegungsdaten genutzt werden. Die Daten werden mit einer zweidimensionalen, also „flachen“ Struktur nach SAP BW transferiert (d. h. als Tabelle und nicht als multidimensionale Datenstruktur). In DataSources befinden sich die Definitionen der Quelldaten.

Dabei werden zwei Feldstrukturen voneinander unterschieden: **Extraktionsstruktur** und **Transferstruktur**. Die Extraktionsstruktur enthält sämtliche Felder des Quellsystems, die von sog. Extraktoren bereitgestellt werden. Extraktoren sind Programme, die Daten aus Quellsystemen sammeln. Während der Extraktion wird der Inhalt der Felder an die Transferstruktur übergeben.

Die Transferstruktur stellt eine Auswahl der Felder einer Extraktionsstruktur des Quellsystems dar.

Beim Daten-Upload werden die Daten 1:1 von der Transferstruktur des Quellsystems in die Transferstruktur des SAP BW übernommen und dann mit Hilfe der Transferregeln (Transfer Rules) in die Kommunikationsstruktur des SAP BW übertragen. Transferregeln dienen dazu, die Daten von der DataSource in die InfoSource zu übertragen und dabei eventuell zu transformieren und zu modifizieren. Mithilfe dieser Transferregeln können die Felder der DataSource den InfoObjects zugeordnet werden, aus denen sich die InfoSource zusammensetzt. Dazu steht eine reichhaltige Bibliothek mit Transformationsfunktionen zur Verfügung, die die Geschäftslogik repräsentieren

InfoSources können sowohl Bewegungsdaten als auch Stammdaten enthalten. Mit Bewegungsdaten werden die Transaktionen nachverfolgt, die in einem OLTP-System (Online Transaction Processing) wie z. B. SAP R/3 vollzogen werden. Sie sind „quantifizierbar“ und können hochgradig granular sein. Stammdaten sind die Daten, die über lange Zeit nicht geändert werden, wie Kundenadressen oder die Organisationsstruktur des Unternehmens.

Bei der Pflege der Übertragungsregeln legen Sie fest, ob die Kommunikationsstruktur aus Feldern der Transferstruktur, mit fixen Werten oder über eine lokale Konvertierungsroutine gefüllt wird.

Konvertierungsroutinen sind ABAP-Programme, die Sie selber anlegen können. Die Routine bezieht sich immer nur auf ein InfoObject der Transferstruktur.

Sie gelangen zu der Pflege der Transferstruktur über den InfoSource-Baum der Administrator Workbench. Das Kontextmenü des zu einer InfoSource gehörenden Quellsystems bietet Ihnen den Abprung zur Pflege über die Funktion *Übertragungsregeln pflegen*.

Es gibt verschiedene Methoden der Übertragung:

- Daten werden 1:1 übertragen (keine Manipulation der Daten)
- Die Felder der Kommunikationsstruktur können mit einer Konstanten bestückt werden
- Durch eine lokale ABAP Routine können Übertragungsregeln flexibel gestaltet werden.

Es besteht die Möglichkeit einer Datenverschlüsselung mit Hilfe der SSF (Secure Store Forward) Schnittstelle. Diese kann mit Hilfe einer ABAP-Routine angebunden werden. Natürlich

kann man aber auch mit einer ABAP-Routine ganze Daten anonymisieren bzw. pseudonymisieren.

2.5.2 Anonymisierung bei Query-Erstellung

Die Abfrageentwicklung (Query Design) ermöglicht grafische und hochgradig interaktive Analyseanwendungen und Reports schnell zu erzeugen und bereitzustellen. Der Query Designer innerhalb von mySAP BI definiert, wie der Benutzer Daten analysieren kann, welche Informationen angezeigt werden können (Autorisierung) und welche Form der Interaktion (Navigation) möglich ist. Die Parametrisierung ermöglicht die Personalisierung von Abfragen in einer Weise, dass eine Query von mehreren Benutzern verwendet werden kann.

Bei der Query-Erstellung kann man auf InfoObjects verzichten, welche nicht angezeigt werden sollen. Aber mit Hilfe der Berechtigungskonzeptes ist es möglich, seine Query zu erstellen und später bei der Ausführung Einschränkungen vorzunehmen, d.h. man kann bestimmte Spalten ausblenden, ein *Drill down* nur bis zu einem gewissen Grad zulassen. Durch die Verwendung von Hierarchien ist es möglich, bestimmte Einstellungen zu hinterlegen.

2.5.3 Datenalterung und Archivierung

Bei einem durchdachten Data-Warehousing-Konzept ist auch eine Strategie zum Thema Datenalterung notwendig.

Es geht hier nicht nur um die Reduzierung der Kosten (Aufbewahrung und Performance), sondern auch um die Beachtung von Lösch- bzw. Aufbewahrungsfristen. Die Daten dürfen nicht unbegrenzt anwachsen. Zwar haben auch ältere Daten, auf die seltener zugegriffen wird, ihre Daseinsberechtigung für Analysezwecke. Sie sollten jedoch auch aus Datenschutzgründen auf das notwendige Volumen reduziert werden. Auch hier sollte die Chance genutzt werden, einen eventuell noch vorhandenen Personenbezug bei Altdaten zu entfernen.

Mit dem Archiving Development Kit (ADK) können InfoCubes und ODS-Objekte in Archivdateien verwandelt und mit den Archivierungstechnologien von Drittanbietern gespeichert werden, wie beispielsweise in optischen Speicher- und hierarchischen Speicherverwaltungssystemen.

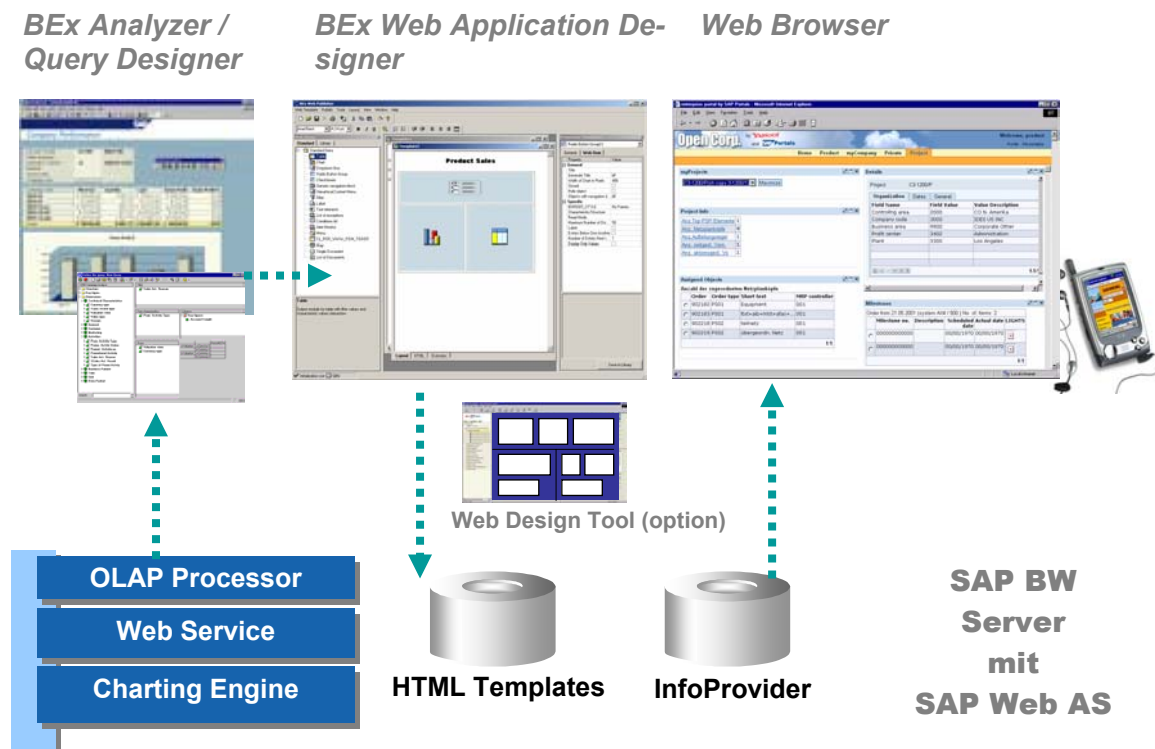
Die ADK-basierte Archivierung erfolgt unabhängig von den zugrunde liegenden Tabellen. Durch das Verschieben von Daten aus SAP BW in unabhängige Speichersysteme können kürzere Lade- und Abfragezyklen sowie signifikante Kosteneinsparungen von bis 90% aufgrund der geringeren Plattenspeicheranforderungen erzielt werden. Für Analysen müssen die archivierte Daten erneut ins SAP BW geladen werden.

2.6 Sichten / Auswertungen

2.6.1 Auswertungswerkzeuge

Die Grundidee des SAP BW ist es, Informationen über entscheidungsrelevante Vorgänge für nahezu alle Funktionen im Unternehmen bereitzustellen. Dazu beinhaltet das SAP BW mit den Reporting-Werkzeugen die Business Explorer Tools, um zentral gespeicherte Daten, die aus verschiedenen Quellen stammen können, auszuwerten und zu präsentieren.

Business Explorer Web Application Framework



Mit den Business Explorer Tools können,

- Reports erstellt,
- vordefinierte Reports ausgeführt,
- berechnete und eingeschränkte Kennzahlen (z.B. Key Performance Indicator) definiert und

- Daten analysiert und präsentationsgerecht aufbereitet werden.

Folgende Komponenten / Werkzeuge des Business Explorer stehen für unterschiedliche Benutzertypen und unterschiedliche Zielsetzungen zur Verfügung:

BEx - Query Designer

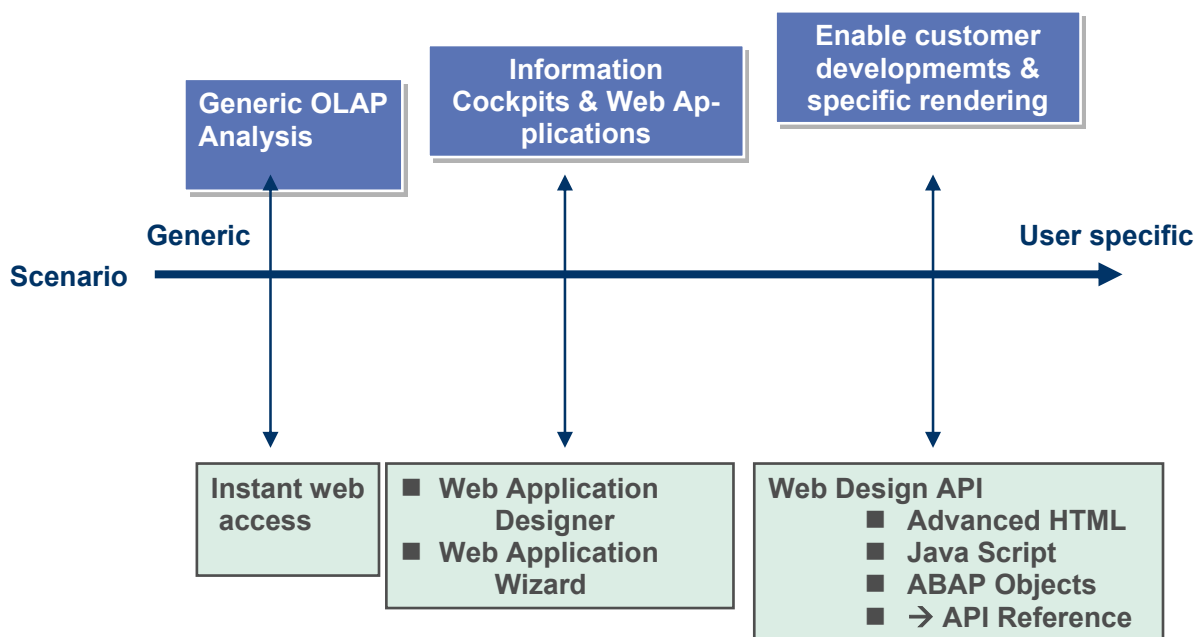
Hiermit können Auswertungen, so genannte Queries über alle im BW hinterlegten Daten erzeugt werden. Der Query Designer kann über das Web oder MS Excel aufgerufen oder als Desktop-Anwendung definiert werden.

BEx Web Application Designer

Der BEx Web Application Designer (SAP BW 3.0B) und der darin integrierten Web Application Wizard erlauben es, individuelle Web Applications zu definieren. Mit Hilfe von Queries und HTML-Dokumenten können Informationen zur Veröffentlichungen im Intranet oder Internet erstellt und präsentiert werden.

Die folgende Übersicht zeigt das breite Spektrum des BEx Web Application Designs:

BEx Web Continuum



BEx Analyzer

Die mittels des BEx Query Designer erstellten Auswertungen können für Excel über den BEx Analyzer zur Verfügung gestellt und z. B. für Präsentationen weiter aufbereitet werden.

BEx Browser

Dieser ist ein Reporting-Menü (ähnlich einem Portal), von dem aus der Endanwender Analysen der anderen Business Explorer-Tools aufrufen kann.

Formatiertes Reporting

Im Rahmen des *formatierten Reporting* erfolgt eine Integration von Crystal Decisions in das BW. Mit diesem Reporting können Berichte mit pixel-genauen Layouts - etwa für vorgegebene Formulare - erstellt werden.

Zugriff auf die Berichte

Die mit den verschiedenen BEx-Werkzeugen erstellten Berichte lassen über so genannte i-Views sehr einfach in ein Portal integrieren.

2.6.2 Auswertungsmöglichkeiten

Die in einem Bericht benötigten Kennzahlen und Merkmale eines oder mehrerer InfoProvider werden mittels Drag & Drop zur Verfügung zusammengestellt.

Zur Navigation in multidimensionalen Datenstrukturen wie den InfoCubes werden die Grundfunktionen **Drill-down** bzw. **Drill-up** verwendet. Unter *drill-down* versteht man die Möglichkeit, die verdichteten Daten entsprechend ihrer Hierarchieebene in die zugrundeliegenden Teilergebnisse zu zerlegen. Der Endanwender kann mithilfe von Navigation durch die verschiedenen Hierarchieebenen von verdichteten Daten gelangen (*Drill-down*) und umgekehrt (*Drill-up*).

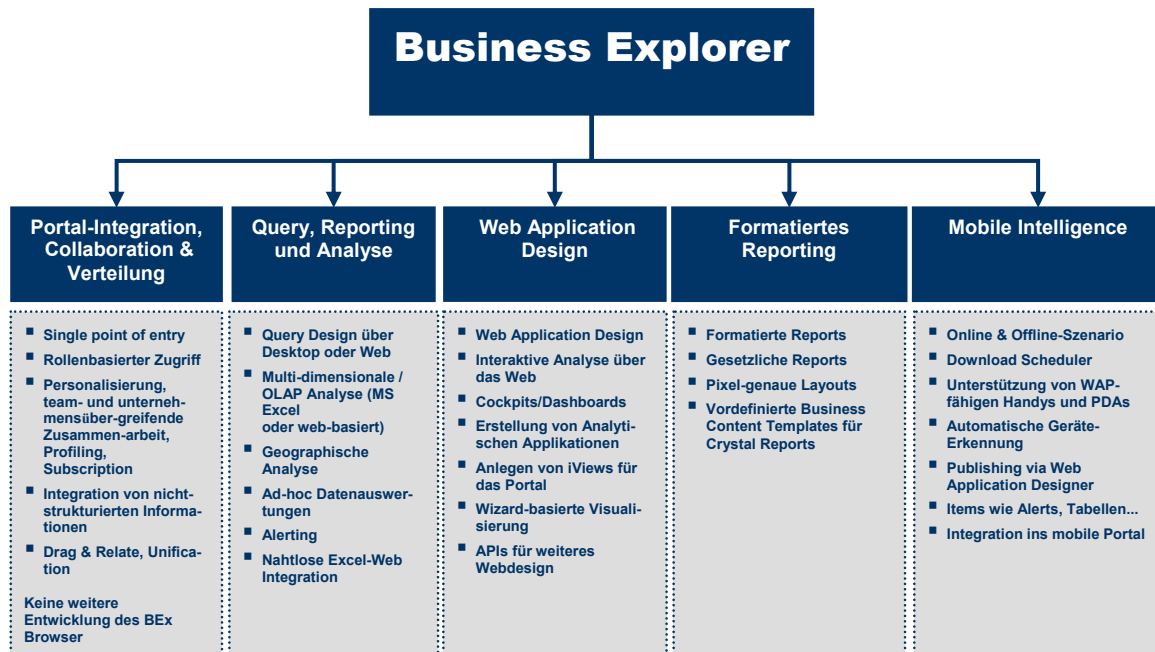
Zusätzlich zu den bisher erläuterten Navigationsfunktionen ist es auch möglich, von einem Report in einen anderen Report zu navigieren, der auf dem selben oder einem anderen InfoCube basiert (**Drill-across**).

Die **Drill-through**-Funktionalität erlaubt einen Durchgriff vom Reporting auf den operativen Datenbestand. Zum einen kann von einem Report aus auf den operativen Datenbestand gespeicherte Belegebene gesprungen werden, zum anderen kann von dort aus direkt auf die zugrunde liegende Transaktion einer SAP-Komponente zugegriffen werden.

Personenbezug

Für das Laden eines Data Warehouses ist zu prüfen, ob personenbezogene Daten im Detail hierfür extrahiert werden müssen. Wird dies seitens des Unternehmens als notwendig erachtet, muss beispielsweise durch Zugriffsberechtigungssteuerung sichergestellt werden, dass nur berechnigte Endbenutzer auf personenbezogene Datenbestände zugreifen dürfen. *Drill down* oder *Drill through* Funktionalitäten auf Einzelpersonen sollten nur berechtigten Endbenutzer erlaubt werden.

2.6.3 Zugriffsrechte bei selbstentwickelten Auswertungen



Die Berechtigungsprüfung auf Datenebene findet im SAP BW statt.

Bei der *Portal-Integration* von Auswertungen/Sichten auf die InfoSources und InfoCubes werden die Daten/Auswertungen in das jeweilige Portal aufgenommen und gegebenenfalls über entsprechende Verknüpfungen im Portal mit anderen Daten des Portals verknüpft.

Ein Zugriffsschutz wird in diesem Falle zusätzlich über die Rollen des jeweiligen Portals gesteuert. **Der Datenschutzverantwortliche muss sich in diesem Falle also zusätzlich um die zu definierenden Rollen des Portals und die definierten *Drag and Relate*-Korrelationen kümmern.**

Im Falle der oben bereits erwähnten *Queries und Sichten* werden die lesenden Zugriffe auf die InfoCubes und InfoObjects durch Queries über spezielle Berechtigungsobjekte geschützt. Der ändernde Zugriff auf Queries wird über die Berechtigungsobjekte S_RS_COMP und S_RS_COMP1 gesteuert. Auch das Anlegen und Ändern der Zuordnung von Queries zu Benutzergruppen wird über diese Berechtigungsobjekte gesteuert. Das Anlegen und Ändern von Sichten auf InfoCubes wird über die Objekte S_RS_ICUBE und S_RS_IOBJ vorgenommen.

Mit diesen Stellschrauben lässt sich

- das Anlegen/Ändern/ Einschränken von Sichten auf die Daten,
- das Erstellen/Ändern von Queries und das Zuordnen von Queries zu Benutzern, sowie
- das reine Abrufen fest vorgegebener Abfragen

auf unterschiedliche Rollen im Rahmen eines 4 oder 6 Augenprinzips verteilen.

Der Datenschutzverantwortliche hat sich in diesem Falle um die abstrakte Rollenaufteilung und um die konkrete Ausgestaltung der entsprechenden Rollen zu kümmern.

Mit Hilfe des BEx Web Application Designers werden *Web Applications* erstellt. Hiermit können HTML Seiten erzeugt werden, die BW spezifische Inhalte, bzw. Tabellen, Charts oder Karten enthalten. Die Web Applications können als URL gesichert und über Internet, Intranet oder mobile Endgeräte darauf zugegriffen werden. Werden die Web Applications als iView gesichert, können sie in Unternehmensportale integriert werden.

Der Zugriffsschutz über die so erstellten Web Applications erfolgt über die Standard-BW-Berechtigungsobjekte (s. Kap. 2.7.2.3). Das Werkzeug, der Web Application Designer selbst, kann über das Berechtigungsobjekt S_RS_TOOLS abgesichert werden, dazu ist allerdings eine kleine Modifikation notwendig (s. Hinweis 605417).

Im Falle des Einsatzes von mobilen Endgeräten zusammen mit dem Werkzeug *BEx Mobile Intelligence* können mit dem BEx Web Application Designer erstellte Auswertungen auch von unterwegs abgerufen werden. Eine Berechtigungsprüfung findet dabei über die Standard-BW-Berechtigungsobjekte statt (s. Kap. 2.7.2.3).

Schließlich sind neben den online verfügbaren Business Explorer Auswertungen mit *Web Applications* und *Mobile Applications* auch offline abrufbare Auswertungen möglich. Mit dem sogenannten BEx Download Scheduler können vorberechnete HTML Seiten auf einen Desktop PC, bzw. ein PDA Gerät heruntergeladen werden. Eine Berechtigungsprüfung findet dabei über die Standard-BW-Berechtigungsobjekte statt (s. Kap.2.7.2.3). Auf dem Frontend gespeicherte Daten müssen mit den jeweiligen lokalen Mitteln geschützt werden (z.B. Verschlüsselung, Passwortschutz).

2.6.4 Auswertungen des Business Content

Ergänzend zu dem in Kapitel 2.1.6 beschriebenen Funktionsumfang des Business Content sollen in diesem Abschnitt die Auswertungsmöglichkeiten und Rollen (denen im BC Queries zugeordnet sind) exemplarisch dargestellt und unter den rechtlichen Anforderungen an ein DataWarehouse betrachtet werden.

Der Vorteil dieser programm- und datentechnischen „fertigen“ Lösung besteht in erster Linie in der Nutzung schon vorhandener Informationsmodelle.

Unter dem Aspekt der datenschutzrechtlichen Anforderungen an ein BW, kann jedoch keineswegs von einer „fertigen“ Lösung gesprochen werden.

In den Informationsmodellen des BC befinden sich sehr viele personenbezogene und/oder personenbeziehbare Daten (z.B. Verkäufergruppe und Vertriebsbeauftragter in der Ergebnisrechnung (CO – PA), Arbeitsplatz mit Ist – und – Soll - Mengen, mit exakten Durchlauf -/ Durchführungszeiten, mit Soll- und Ist – Zeitgraden, mit einzelnen Arbeitsvorgängen etc.).

Es besteht das datenschutzrechtliche Risiko, dass BW Anwender die „fertigen Lösungen“ des BC übernehmen, ohne sie einer weiteren (datenschutz-) rechtlichen Prüfung der Zulässigkeit zu unterziehen.

Um diesen Sachverhalt zu verdeutlichen, wird im Folgenden auf einige ausgewählte Beispiele verwiesen. Ziel ist dabei nicht die vollständige Auflistung aller Queries, die personenbezogene Daten verarbeiten. Wir weisen nachdrücklich darauf hin, dass bei Einsatz des Business Content

- die Zulässigkeitsvoraussetzung der Daten im operativen System durch die verantwortliche Stelle geprüft werden muss
- die Verarbeitung im Rahmen der ursprünglichen Zweckbestimmung noch gegeben sein muss
- geprüft werden muss, ob durch Kombinationsmöglichkeiten von Daten des Business Content neue Zwecksetzungen verfolgt werden können
- das Berechtigungskonzept auf personenbezogene Daten zwischen dem operativen System und dem BW Business Content ggf. 1 : 1 abgebildet worden ist

Der BC enthält z.Zt. zu folgenden Anwendungen Informationsmodelle – und damit auch Queries (Auswertungen) – im o.g. Sinne (Stand ist BW Release 3.0 A) :

- Analytische Applikationen
- Customer Relationship Management
- Supplier Relationship Management
- Supply Chain Management
- Product Life – Cycle Management
- Financials
- Human Ressources
- Exchanges
- Industry Solutions (dort für 17 Branchen)
- Country – Specific Content
- Demo Content
- Anwendungsübergreifende Komponenten

Für diese Bereiche sind o.g. Informationsmodelle mit i.d.R. folgender Struktur hinterlegt :

- Rollen
- Queries
- InfoSources
- DataSources
- InfoCubes
- ODS – Objekte
- Kennzahlen
- Merkmale

- Arbeitsmappen

Eine vollständige Aufzählung der personenbezogenen Daten würde den Rahmen dieses Leitfadens sprengen.

Im Folgenden beschränken wir uns auf eine exemplarische Behandlung von „nicht HR“ und „HR“-Queries als BC

Im SAP BW gibt es ähnliche Techniken zum Auffinden personenbezogener Daten wie im R/3. Im R/3 werden die Tabellen mit Personenbezug über Domänen mit dem ABAP Dictionary analysiert, im SAP BW werden die Informationen aus den InfoObjects mit dem Administrator Workbench ermittelt, z.B. *ovendor*, *ocustomer*, *oemployee*. Ähnlich wie beim ABAP Dictionary gibt es auch hier Verwendungsnachweise.

Da der Administrator Monitor Workbench ein privilegiertes Werkzeug der Administration ist, empfehlen wir diese Funktionen auch von dieser durchführen zu lassen.

2.6.4.1 Beispiele aus nicht HR-Anwendungen

DemoCube Ergebnisrechnung (CO – PA) (technischer Name : 0D_CO_PA)

Der DemoCube der Ergebnis- und Marktsegmentrechnung (CO-PA) dient als Datenbasis für beispielhaft ausgelieferte DemoQueries für Auswertungen im Vertriebscontrolling.

Die Query enthält personenbezogene Daten wie z.B. „Verkäufergruppe“ (0D_SALE_GRP), die in Verbindung mit Absatzmenge (0D_QTY) eine Leistungsmessung/-bewertung ermöglicht und evtl. Mitbestimmungsrechte tangiert.

PSP – Element : Kosten/Abweichungen (technischer Name : OPS_C01_Q0002)

Diese Query bietet einen Überblick über die auf einem PSP-Element angefallenen Kosten. Sie ermöglicht die Analyse dieser Kosten im Ist und Plan nach Kostenarten und gibt die Abweichung von den Plankosten absolut in der jeweiligen Währung und in Prozent an.

Abhängig vom Detaillierungsgrad der PSP – Elemente (ein PSP – Element ist einer Person zugeordnet), kann hier ein Personenbezug bestehen, der zusätzlich eine Leistungskontrolle ermöglicht.

Überblicksbericht – Projekte (technischer Name : OPS_C01_Q0004)

Mit Hilfe dieser Query erhalten Sie einen Überblick über den Entwicklungsstand der von Ihnen selektierten Projekte. Die Query vergleicht Ist- und Plankosten, Ist- und Planarbeit und Eckstart- und Eckendtermine der selektierten Projekte.

Unter den beim PSP-Element beschriebenen Rahmenbedingungen sind auch hier personenbezogene Daten vorhanden und eine Leistungsmessung/-bewertung ist möglich, die evtl. Mitbestimmungsrechte tangiert.

Zeitgrad (technischer Name : OPP_C03_Q011)

Diese Query stellt die Soll - Zeitgrade und die Ist – Zeitgrade am Arbeitsplatz gegenüber. Sie zeigt damit an, wie effektiv an einem Arbeitsplatz gearbeitet wird.

Kann einem Arbeitsplatz eine Person oder eine (kleine) Gruppe von Personen zugeordnet werden, handelt es sich um personenbezogene Daten, die eine Leistungsmessung/-beurteilung ermöglichen und somit Mitbestimmungsrechte tangieren.

Ist – Mengen am Arbeitsplatz (technischer Name : OPP_C04_Q002)

Diese Query stellt die angelieferte Losgröße, die rückgemeldete Menge und den rückgemeldeten Ausschuss periodengenau dar.

Es wird auf die Ausführungen der o.g. Beispiele verwiesen.

Diese wenigen Beispiele – auch von direkt personenbezogenen Daten – aus den Bereichen Business Content,

- Product Life Cycle Management
- Programm & Projektmanagement

und

- Supply Chain Management
- Fertigung

zeigen die Notwendigkeit, den BC vor seiner Nutzung rechtlich zu prüfen, zu bewerten und die entsprechenden Maßnahmen wie z.B. Anonymisierung, Pseudonymisierung, Überprüfen und evtl. Anpassen des Berechtigungskonzeptes einzuleiten und umzusetzen.

2.6.4.2 Business Content für HR-Daten

Die mehrdimensionalen Sichtweisen im SAP BW ermöglichen es mit einer einzigen mySAP HR-Query viele klassische Standardreports abzudecken.

So beinhaltet der mySAP HR-Business Content z.B. die Abbildung des Personalbestandes auf organisatorische Merkmale, wie die Organisationsstruktur des Unternehmens, die Mitarbeitergruppen, die Personalbereiche und die Kostenstellen. Zusätzlich werden personenbezogene Merkmale wie Geschlecht, Alter oder Nationalität dargestellt.

Durch die freie Kombination aller Merkmale mit dieser Query, ist eine detaillierte Informationsdarstellung bis auf den einzelnen Mitarbeiter hinunter möglich.

Eine Rechtsgrundlage für die Speicherung und Nutzung dieser Daten für alle mit diesen Werkzeugen möglichen Zwecke muss vorliegen. Die SAP-AG hat dies nicht geprüft. Liegt die Rechtsgrundlage nicht vor, sind die Daten zu aggregieren, anonymisieren oder zu pseudonymisieren.

Die Aufgabe des Datenschutzbeauftragten besteht beim Business Content im HR weiter darin, darauf hinzuwirken, dass konzernweit bei der Personalplanung nur aggregierte Daten über Personalbestand, Personalbewegungen oder Mitarbeiterstruktur übermittelt werden. Persönliche Details wie z.B. Alter, Geschlecht, Nationalität, Skills oder Ausbildung haben in den Quellsystemen zu verbleiben.

Ein weiterer zentraler Punkt ist das Benutzerberechtigungskonzept (s.a. Kapitel 2.8.2.4.).

Die im Business Content HR vorhandenen „Standardrollen“ sind – im Gegensatz zu den sehr allgemein gehaltenen Standardrollen im „allgemeinen“ BW – spezifisch auf Aufgaben zugeschnitten und enthalten die für diese Rolle notwendigen Queries.

Für die Rolle Controller Personalzeiten ist hier exemplarisch die Datenschutzrelevanz von „vorgefertigten“ Auswertungen und Rollen im Business Content HR dargestellt :

Controller Personalzeiten (Technischer Name: SAP_BW_0ROLE_0024)

Der *Controller Personalzeiten* stellt Daten bereit, die eine Überwachung der Personalzeiten im Hinblick auf strategische Unternehmensziele ermöglichen. Er erstellt Berichte z.B. über das Arbeitsaufkommen aller Abteilungen/Mitarbeitergruppen oder die Entwicklung des Mehrarbeitsaufkommens.

Auswertungen dieses Datenmaterials ermöglichen z.B. die Steuerung des Mehrarbeitsaufkommens und der Produktivität einzelner Unternehmensbereiche.

Die Rolle umfasst u.a. die folgenden Aktivitäten in der Personalzeitwirtschaft:

- Statistiken über Fehlzeiten, Produktivität und Mehrarbeitsaufkommen erstellen
- Urlaubsreste und weitere Ansprüche auf bezahlte Fehlzeiten analysieren

Für die Aufgaben des *Controller Personalzeiten* stehen folgende Arbeitsmappen zur Verfügung. Jeder Aufgabe entspricht ein Cluster aus mehreren Arbeitsmappen. Die Arbeitsmappen enthalten eine oder mehrere Queries, die die relevanten Informationen liefern.

Aufgabe (Cluster)	Arbeitsmappe
Kennzahlen zu Personalzeiten	Kostenstellenbelastung im Jahresvergleich
	Personalzeiten Monatsentwicklung
	Personalzeitenüberblick im Vergleich zum Vorjahr
	Personalzeiten ausgedrückt in Vollzeitkräften
Übersichten zu Personalzeiten	Produktivitätsrate
	Mehrarbeitsrate
	Krankheitsrate
	Urlaub pro Soll
	Genommener Urlaub pro effektiver Vollzeitkraft

Diese Arbeitsmappen ermöglichen – wenn nicht bei der Anpassung der Rollen eingeschränkt – den Drill-Down auf einzelne Beschäftigte.

Als erstes muss die mehrfach angesprochene Frage nach der Zulässigkeit von diesen personenbezogenen Daten geklärt werden. Erweist sich die Zulässigkeitsvoraussetzung als nicht erfüllt, dürfen diese Daten im BC HR nicht verarbeitet und genutzt werden.

Ergibt sich ein Erlaubnistatbestand, ist zu prüfen, ob die im BC angebotenen Rollen die tatsächlichen organisatorischen und aufgabenspezifischen Gegebenheiten des Anwenderunternehmens überhaupt wiedergeben, oder ob die Berechtigungen die mit dieser Rolle ausgeliefert werden nicht viel zu weit gefasst sind. „Einschränkungen“ der Berechtigungen z.B. auf bestimmte Personalbereiche oder Mitarbeitergruppen etc. sind erforderlich.

Folgende Rollen sind zur Zeit im Business Content HR vorhanden (Grundlage Dokumentation SAP BW Release 3.0A 2001) :

- **Personalbeschaffer** (Technischer Name: OROLE_0020)

Die Rolle des *Personalbeschaffers* umfasst alle administrativen Tätigkeiten und Datenerfassungen im Bereich der Komponente *Personalbeschaffung*.

- **Personalcontroller** (Technischer Name: OROLE_0021)

Der *Personalcontroller* wird als strategischer Geschäftspartner der Personal- und Unternehmensleitung verstanden. Er verfügt über ein ausgeprägtes Fachwissen und weiß die HR- Politik nach den strategischen Zielen des Unternehmens auszurichten.

- **Leiter Personalabrechnung** (Technischer Name: OROLE_0023)

Der *Leiter Personalabrechnung* ist verantwortlich für den kompletten Bereich der Abrechnung (Ablauf, Überwachung, Folgeaktivitäten usw.).

Kennzahlen und Auswertungen aus der Personalabrechnung unterstützen ihn bei Analysen und bei der anschließenden Entscheidungsfindung.

- **Experte Arbeitgeberleistungen** (Technischer Name: OROLE_0027)

Der *Experte Arbeitgeberleistungen* wird als strategischer Geschäftspartner des Personalleiters und der Fachvorgesetzten verstanden. Er verfügt über ein ausgeprägtes Fachwissen und weiß die Personalpolitik nach den strategischen Zielen des Unternehmens auszurichten. Er löst Probleme anhand von HR-basierten Lösungsansätzen und ist bei der betrieblichen Umsetzung maßgeblich beteiligt.

- **Organisationsplaner** (Technischer Name: OROLE_0025)

Der *Organisationsplaner* wird als strategischer Geschäftspartner des Personalleiters und der Fachvorgesetzten verstanden. Er verfügt über ein ausgeprägtes Fachwissen und weiß die Personalpolitik nach den strategischen Zielen des Unternehmens auszurichten. Er löst Probleme anhand von HR-basierten Lösungsansätzen und ist bei der betrieblichen Umsetzung maßgeblich beteiligt.

Er ist ebenso verantwortlich für Systemprozessanalyse und -design. Im Mittelpunkt stehen dabei Qualitätsverbesserungen, Data Management, Prozessverbesserungen und/oder Re-Engineering.

- **Experte Training** (Technischer Name: OROLE_0022)

Der *Experte Training* wird als strategischer Geschäftspartner des Personalleiters und der Fachvorgesetzten verstanden. Er verfügt über ein ausgeprägtes Fachwissen im Bildungsbereich und weiß die Aus- und Weiterbildung nach den strategischen Zielen des Unternehmens auszurichten. Der Experte ist verantwortlich für alle Planungsaufgaben und die Gesamtkoordination der Bildungsaktivitäten im Unternehmen. Wichtig ist in diesem Zusammenhang die Auswertung relevanter Bildungsdaten.

- **Personalentwickler** (Technischer Name: OROLE_0028)

Der *Personalentwickler* ist ein Experte in der *Personalentwicklung* und wird als strategischer Geschäftspartner des Personalleiters und der Fachvorgesetzten verstanden. Er verfügt über ein ausgeprägtes Fachwissen und weiß die Personalentwicklung nach den strategischen Zielen des Unternehmens auszurichten. Die generelle Aufgabe ist es, strategische Unternehmensvorgaben in Personalentwicklungskonzepte und Lösungsansätze zu übertragen und umzusetzen. Wichtig ist in diesem Zusammenhang die Auswertung relevanter Daten der Personalentwicklung (d.h. zu Qualifikationen und Beurteilungen).

- **Experte Vergütungsmanagement** (Technischer Name: OROLE_0026)

Der *Experte Vergütungsmanagement* entwickelt und leitet die Einführung von Vergütungsprogrammen, die den Mitarbeitern eine wettbewerbsfähige Bezahlung, Motivation und Belohnung bieten.

Im Mittelpunkt stehen Programme für monetäre Bezahlung (Gehalt, Bonus) und Programme für geldähnliche Bezahlung (Unternehmensbeteiligungspläne) für Arbeiter und Angestellte

- **Personalkostenplaner** (Technischer Name: OROLE_0030)

Der *Personalkostenplaner* ist für die Analyse verschiedener Kostenszenarien zuständig. Die Kennzahlen und Auswertungen aus der Personalkostenplanung unterstützen ihn bei Analysen und bei der anschließenden Entscheidungsfindung.

- **Employee Relations Manager** (Technischer Name: SAP_BW_OROLE_0029)

Der *Employee Relations Manager* führt Verhandlungen mit Arbeitgebern, Arbeitnehmern und Gewerkschaften. Seine Aufgabe besteht in der Aushandlung und Festlegung von Lohnniveaus, in der Darstellung von Protokollen und Berichten und in der Beratung und Schulung von Führungskräften in den Bereichen Betriebsrats- bzw. Gewerkschaftsarbeit.

Die Rolle *des Employee Relations Managers* hat eine Asien- bzw. US-spezifische Ausprägung. In anderen Ländern, z.B. Deutschland, können die Aufgaben oder Teile der Aufgaben des *Employee Relations Managers* durch den Personalreferenten, den Gewerkschafts- oder Betriebsratsvertreter wahrgenommen werden.

- **Reisemanager** (Technischer Name: OROLE_0032)

Das Reporting des BW Business Content unterstützt den Reisemanager bei der Auswertung der Daten zu geplanten und durchgeführten Reisen und deren Abrechnung. Durch den Einsatz des BW erhält er z. B. sofort problemlos Informationen zu Reise-

destinationen, Umsätzen mit Hotelketten und Mietwagengesellschaften oder Statistiken der Spesenbelege.

- **HR BW Web Cockpits** (Technischer Name: SAP_BW_0ROLE_0019)

Diese Rolle steht Ihnen aus technischer Sicht zur Verfügung, um einem Benutzer die Web Cockpits der *Personalwirtschaft* (HR) zuzuordnen. Die HR-Web-Cockpits liefern u.a. Business Content für das Business Package *Manager Self-Service*.

Sicherzustellen ist, dass diese Rollen den vorhandenen Aufgaben des Anwenders entsprechen. Allgemeine, mit sehr weitgehenden Rechten ausgestattete Rollen sind zu vermeiden. Datenschutzverantwortliche müssen dafür Sorge tragen, dass diese Rollen mit ihren Berechtigungen den betrieblichen Realitäten und Gegebenheiten angepasst werden, um die Zulässigkeitsvoraussetzungen zu erfüllen bzw. das Gebot der Zweckbindung und dessen technischer Sicherstellung zu gewährleisten.

Der im Kapitel 2.5.1 beschriebene ETL (Extrahieren, Transformieren und Laden) Prozess ist ein wichtiger Zeitpunkt für die Verantwortlichen zur Prüfung der Zulässigkeit der Verarbeitung und Nutzung der Daten.

2.7 Umsetzung der Anforderungen aus § 9 BDSG und Anlage: technisch-organisatorische Maßnahmen

2.7.1 Anforderungen

In diesem Abschnitt werden die technisch-organisatorischen Anforderungen an die Erfassung, Verarbeitung und Nutzung personenbezogener Daten und deren Prüfungen behandelt. Die Anforderungen sind allgemein, d.h. insbesondere auch bei der Verarbeitung außerhalb des Geltungsbereichs nationaler Gesetze zu erfüllen. Diese Vorschriften beziehen sich nicht allein auf Produktivsysteme, sondern auch auf vorgelagerte Systeme, soweit dort personenbezogene Daten zugreifbar sind oder dort Einstellungen vorbereitet werden, die später in die Produktionsumgebung transportiert werden.

Neu ist auf Grund der EU-Richtlinie 95/46/EG die Ausweitung der erforderlichen technisch-organisatorischen Maßnahmen auf solche, die einerseits Schutz gegen die zufällige oder unrechtmäßige Zerstörung und den zufälligen Verlust der Daten bieten (Ziffer 7: Verfügbarkeitskontrolle) und die andererseits die Zweckbindung der Verarbeitung gewährleisten (Ziffer 8).

Verweis: Die geltenden gesetzlichen Anforderungen aus § 9 BDSG sowie eine Übersicht zur SAP-Funktionalität zur Abdeckung dieser Anforderungen findet sich im Kapitel 4.1. des *Leitfadens Datenschutz für SAP R/3*. Eine Übersicht zum Zusammenhang zwischen den beiden Leitfäden ist in 2.7.2.11 enthalten.

2.7.2 SAP-Fakten, Risiken und Maßnahmen

2.7.2.1 Identifizierung und Authentifizierung

Bevor ein Benutzer auf die Informationen und Funktionen im R/3-System zugreifen kann, muss er sich über ein entsprechendes Logon mittels einer Benutzer-ID und einem Kennwort anmelden. Im Gegensatz zu den Administratoren melden sich die Endbenutzer in der Regel nicht direkt im Business Warehouse an, sondern erhalten über ein Portal oder über ein Frontend den benötigten Zugang. Durch die Eingabe der Authentifizierungsdaten identifiziert sich der Anwender gegenüber R/3 und das System kontrolliert, ob der Benutzer berechtigt ist, mit dem System zu arbeiten.

Verweis: Die hierbei geltenden Regeln sowie Hinweise für entsprechend sichere Einstellungen zur Kennwortgestaltung sind im Kapitel 4.2.1. des *Leitfadens Datenschutz für SAP R/3* beschrieben. Zusätzlich sind bei Einsatz eines Portals weitergehende Maßnahmen bezüglich der Authentifizierung zu treffen und zu überwachen.

2.7.2.2 Standardbenutzer

Innerhalb des BW gibt es wie im R/3 Classic insgesamt 4 Standardbenutzer (SAP*, DDIC, SAPCPIC, EARLYWATCH), die im Rahmen der zu ergreifenden organisatorisch-technischen Maßnahmen gesondert zu schützen sind.

Verweis: Kapitel 4.2.2. des *Leitfadens Datenschutz für SAP R/3*.

2.7.2.3 Benutzerberechtigungskonzept: Berechtigungsobjekte für BW

Grundsätzliche Zugriffsteuerung

Der Zugriffsschutz für ein BW-System wird auf der Basis von Berechtigungsobjekten aufgebaut. SAP liefert hiervon im Standard ca. 300 aus. Davon sind die Berechtigungsobjekte der folgenden Objektklassen zur Sicherstellung eines wirksamen Berechtigungskonzeptes zum Schutz personenbezogener Daten von besonderer Bedeutung:

Objektklasse	Bezeichnung
AAAB	Anwendungsübergreifende Berechtigungsobjekte
BC_A	Basis – Administration
BC_C	Basis – Entwicklungsumgebung
BC_Z	Basis – Zentrale Funktionen
HR	Personalwesen

RS	Business Information Warehouse
RSR	Business Information Warehouse - Reporting (eigenerstellte Berechtigungsobjekte)

Im Folgenden werden sämtliche Berechtigungsobjekte aus der Objektklasse RS „Business Information Warehouse“ vorgestellt. Die komplette Dokumentation der Berechtigungsobjekte ist über den Menüpfad

Werkzeuge -> Administration -> Benutzerpflege -> Informationssystem -> Berechtigungsobjekte (alle Objekte der Objektklasse RS)

oder über den Profilgenerator (PFCG) ersichtlich.

Berechtigungsobjekte des BW

Generell können bei den spezifischen BW-Berechtigungsobjekten folgende Arten unterschieden werden:

- Einschränkungen innerhalb der Administrator Workbench
- Einschränkungen innerhalb des Business Explorer
- Einschränkungen der Reports auf bestimmte Inhaltsangaben (Transaktion RSSM)

Als Besonderheit für BW Systeme ist hervorzuheben, dass neben den Standardberechtigungsobjekten in Abhängigkeit von den personenbezogenen Daten eigene Berechtigungsobjekte zu erstellen sind. Hierfür steht im System die Transaktion RSSM zur Verfügung.

Die eigenerstellten Berechtigungsobjekte bilden die notwendige Grundlage, um spezifisch für die definierten Informations- und Datenstrukturen - z.B. bezüglich InfoCubes - geeignete technische Maßnahmen zum Zugriffsschutz aufzubauen, um zum Beispiel eine Einschränkung der Zugriffsrechte auf Feldebene zu erreichen. Die Objekte beziehen sich vorrangig auf die Reporting-Funktionen und steuern, dass der Anwender aus dem Gesamtbestand der BW-Informationen ausschließlich die organisatorisch festgelegten personenbezogenen Daten auswerten kann.

Berechtigungsobjekte für	Felder / Einschränkungen
Administrator Workbench	

Berechtigungsobjekte für Administrator Workbench	Felder / Einschränkungen
<p>S_RS_ADMWB</p> <p>Administrator Workbench - Objekte</p> <p><u>Zweck:</u> Einschränken auf bestimmte Objekte innerhalb der Administrator Workbench</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>Anzeigen, Pflegen, Ausführen, Aktualisieren</p> <p><u>Festlegung der zu bearbeitenden Objekte</u></p> <ul style="list-style-type: none"> → Quellsystem → InfoObject → Monitor → Anwendungskomponente → InfoArea → Administrator Workbench → Einstellungen → Metadaten → InfoPackage → Reporting-Agent-Einstellung → Dokumente
<p>S_RS_HIER</p> <p>Administrator Workbench - Hierarchie</p> <p><u>Zweck:</u> Einschränken auf Hierarchieebenen innerhalb der Administration</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>Anzeigen, Pflegen, Auswerten</p> <p><u>Festlegung InfoObject</u></p> <p><u>Festlegung Hierarchienamen</u></p> <p><u>Festlegung Hierarchieversion</u></p>

Berechtigungsobjekte für Administrator Workbench	Felder / Einschränkungen
<p>S_RS_ICUBE</p> <p>Administrator Workbench - InfoCube</p> <p><u>Zweck:</u> Einschränken auf InfoCubes</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>- Anzeigen, Löschen, Pflegen, Aktualisieren</p> <p><u>Festlegung InfoArea</u></p> <p><u>Festlegung InfoCube</u></p> <p><u>Festlegung Teilobjekts zum InfoCube</u></p> <p>→ Definition → Fortschreibungsregeln → Aggregat → Export → Export Datenquelle</p>
<p>S_RS_IOBC</p> <p>Administrator Workbench - InfoObjektCatalogs</p> <p><u>Zweck:</u> Einschränken auf InfoObject Kataloge</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>- Anzeigen, Pflegen</p> <p><u>Festlegung InfoArea</u></p> <p><u>Festlegung InfoCatalogs</u></p>
<p>S_RS_IOBJ</p> <p>Administrator Workbench - InfoObjekt</p> <p><u>Zweck:</u> Einschränken auf InfoObject</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>- Anzeigen, Pflegen</p> <p><u>Festlegung InfoObjectCatalog</u></p> <p><u>Festlegung InfoObject</u></p> <p><u>Festlegung des Teilobjekts zum InfoObject</u></p> <p>→ Definition → Fortschreibungsregeln</p>

Berechtigungsobjekte für Administrator Workbench	Felder / Einschränkungen
<p>S_RS_IOMAD</p> <p>Administrator Workbench - Stammdaten</p> <p><u>Zweck:</u> Einschränken der Stammdatenpflege innerhalb der Administrator Workbench</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>- Anzeigen, Pflegen</p> <p><u>Festlegung InfoObjectCatalog</u></p> <p><u>Festlegung InfoObject</u></p> <p><u>Festlegung des Teilobjekts zum InfoObject</u></p> <p>→ Definition</p> <p>→ Fortschreibungsregeln</p>
<p>S_RS_ISET</p> <p>Administrator Workbench - Infoset</p> <p><u>Zweck:</u> Einschränken auf Infosets</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>- Anzeigen, Pflegen</p> <p><u>Festlegung InfoArea</u></p> <p><u>Festlegung Infoset</u></p> <p><u>Festlegung des Teilobjekts zum Infoset</u></p> <p>→ Definition</p> <p>→ Daten</p>
<p>S_RS_ISOUR-</p> <p>Administrator Workbench - InfoSource Fortschreibung flexible</p> <p><u>Zweck:</u> Einschränken auf InfoSource mit flexibler Fortschreibung</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>- Anzeigen, Pflegen, Anfordern</p> <p><u>Festlegung der Anwendungskomponente</u></p> <p><u>Festlegung InfoSource</u></p> <p><u>Festlegung des Teilobjekts zum Infoset</u></p> <p>→ Definition</p> <p>→ Kommunikationsstruktur</p> <p>→ Übertragungsregeln</p> <p>→ Daten</p> <p>→ Info Package</p> <p>→ Metadaten</p>

Berechtigungsobjekte für Administrator Workbench	Felder / Einschränkungen
<p>S_RS_ISRCM</p> <p>Administrator Workbench - InfoSource direkte Fortschreibung</p> <p><u>Zweck:</u> Einschränken auf InfoSource mit direkter Fortschreibung</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>Anzeigen, Pflegen, Anfordern</p> <p><u>Festlegung der Anwendungskomponente</u></p> <p><u>Festlegung InfoSource</u></p> <p><u>Festlegung des Teilobjekts zum Infoset</u></p> <p>→ Übertragungsregeln → Daten → Info Package → Metadaten</p>
<p>S_RS_MPRO</p> <p>Administrator Workbench - Multiprovider</p> <p><u>Zweck:</u> Einschränken auf Multi Provider</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>Anzeigen, Pflegen</p> <p><u>Festlegung der InfoArea</u></p> <p><u>Festlegung MultiProvider</u></p> <p><u>Festlegung des Teilobjekts zum MultiProvider</u></p> <p>→ Definition → Export DataSource n</p>
<p>S_RS OSDO</p> <p>Administrator Workbench - ODS Objekt</p> <p><u>Zweck:</u> Einschränken auf ODS</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>Anzeigen, Pflegen</p> <p><u>Festlegung der InfoArea</u></p> <p><u>Festlegung ODS Objekt</u></p> <p><u>Festlegung des Teilobjekts zum ODS</u></p> <p>→ Definition → Fortschreibungsregel → Daten → Export DataSource</p>

Berechtigungsobjekte für Business Explorer	Felder / Einschränkungen
<p>S_RS_COMP</p> <p>Business Explorer - Komponenten</p> <p><u>Zweck:</u></p> <p>Einschränken auf bestimmte Komponenten des Business Explorer bei der Query Definition</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>Hinzufügen, Ändern, Anzeigen, Löschen, Ausführen, Eintragen</p> <p><u>Festlegung der InfoArea</u></p> <p><u>Festlegung der InfoProvider</u></p> <p><u>Festlegung der Reporting-Komponente</u></p> <p><u>Festlegung des Komponententyps</u></p> <ul style="list-style-type: none"> → Query (REP) → Strukturen (STR) → berechnete Kennzahlen (CKF) → eingeschränkte Kennzahlen (RKF)
<p>S_RS_COMP1</p> <p>Business Explorer - Komponenten: Erweiterung auf Owner</p> <p><u>Zweck:</u></p> <p>Mit diesem Objekt besteht die Möglichkeit, Queries von bestimmten Besitzern (Anleger der Query) nur gewissen Benutzern zur Anzeige oder Bearbeitung zugänglich zu machen. (in Verbindung mit S_RS_COMP)</p>	<p><u>Festlegung der Zugriffsart</u></p> <p>Ändern, Anzeigen, Löschen, Ausführen, Eintragen</p> <p><u>Festlegung der Reporting-Komponente</u></p> <p><u>Festlegung des Komponententyps</u></p> <ul style="list-style-type: none"> → Query (REP) → Strukturen (STR) → berechnete Kennzahlen (CKF) → eingeschränkte Kennzahlen (RKF) <p><u>Festlegung des Besitzers</u></p>
<p>S_RS_FOLD</p> <p>Business Explorer - Ordner ein oder aus</p> <p><u>Zweck:</u></p> <p>Ein- oder Ausschalten der allgemeinen Sicht auf den Ordner InfoArea.</p>	<p><u>Festlegung der Ordneransicht</u></p> <p>SUP_FOLDER = „X“, um die Drucktaste <i>Ordner</i> auszublenden, sonst Feld leer lassen oder auf „*“ setzen.</p>

Berechtigungsobjekte für Business Explorer	Felder / Einschränkungen
S_RS_TOOLS Business Explorer - einzelne Werkzeuge <u>Zweck:</u> Einschränkung auf bestimmte Benutzerkreise	Festlegung „logical command name“ Derzeit ist das Berechtigungsobjekt ohne Wirkung, die Prüfung kann für den BEx Web Application Designer als Modifikation aktiviert werden (vgl. Hinweise 332738 und 605417).

Berechtigungsobjekte für Reportberechtigungen	Felder / Einschränkungen
S_RSR_...	BW Reportingberechtigung Technik, um Berechtigungen abhängig vom Inhalt im BW zu definieren <ul style="list-style-type: none"> - Berechtigungsvariablen nutzen - InfoObjekts als berechtigungsrelevant kennzeichnen - InfoCubes anschalten - Berechtigungsvariablen in Queries mit aufnehmen - Nutzung der Transaktion RSSM - Besonderheiten bei Hierarchie-Berechtigungen

Systemberechtigungen

Neben den zuvor aufgeführten BW-Berechtigungsobjekten werden bei Transaktionen im BW-System auch systembezogene Berechtigungsobjekte geprüft. Diese sind in den gleichen Objektklassen enthalten, wie sie von Standard-R/3-Systemen bekannt sind. Es bestehen somit hinsichtlich der diesbezüglichen Berechtigungen vergleichbare Risiken und zu treffende Maßnahmen.

Das BW spezifische Debugging-Tool RSRTRACE ist über den Transaktionscode geschützt. Bei der Ausführung werden alle programmierten Berechtigungsprüfungen durchgeführt. Es gelten die gleichen Vorsichtsmaßregeln wie beim Debuggen in einem Standard-R/3 System.

Verweis: *Leitfaden Datenschutz für SAP R/3*, Kapitel 4.2.3.

Es sind in BW Systemen jedoch nicht sämtliche Berechtigungsobjekte vorhanden, wie sie in R/3-Systemen ausgeliefert werden. So steht z.B. das Objekt P_ORGIN (HR-Stammdaten) in BW-Systemen nicht zur Verfügung.

Für ein differenziertes Reporting sind eigenerstellte Berechtigungsobjekte (S_RSR_* bzw. Z*-Objekte) notwendig. In dieser Beziehung unterscheidet sich der Zugriffsschutz bei BW- und R/3-Systemen wesentlich. Bei letzteren stehen im Auslieferungsstandard eine Vielzahl von Berechtigungsobjekten für Reportingfunktionalitäten zur Verfügung. BW-Systeme sind hier von der Architektur her flexibler, so dass für Auswertungen mit den eigenerstellten Berechtigungsobjekten gesonderte technische Maßnahmen notwendig sind. Die Erstellung des BW- Berechtigungskonzeptes erfordert einen entsprechend hohen Aufwand, der im Projekt einzuplanen ist.

Die restriktiv zu gewährenden Zugriffsrechte dürfen nicht durch Systemberechtigungen unterlaufen werden können. Dies sollte bereits bei der Datenmodellierung beachtet werden. Wichtige systemnahe Berechtigungsobjekte sind in diesem Zusammenhang z.B.

- S_TABU_DIS Tabellenpflege bzw. -anzeige (über Standardtools wie z.B. SM30, SE16)

Hinweis: PSA und ODS enthalten die Daten im Klartext, so dass diese mit SE16 gelesen werden können. Dies ist nicht möglich bei den Daten aus dem InfoCube, da diese in INTEGER-Format vorliegen.

- S_DEVELOP Programmierung; es sind alle Queries / ABAPs mit der SE38 änderbar.
- S_TCODE Transaktionscode-Prüfung bei Transaktionsstart
- S_QUERY Berechtigung SAP Query.

Wesentliche unter Datenschutzaspekten bedeutsame Funktionen, wie das Laden der Daten aus dem Quellsystem bzw. mehreren Quellsystemen, die Pflege bzw. die Anzeige von InfoAreas und InfoObjects, können anhand von BW-Berechtigungsobjekten autorisiert werden. Hier sind z.B. die folgenden Berechtigungsobjekte zu nennen:

- S_RS_ADMWB Administrator Workbench - Objekte
- S_RS_HIER Administrator Workbench - Hierarchie
- S_RS_ICUBE Administrator Workbench - InfoCube
- S_RS_IOMAD Administrator Workbench - Stammdaten pflegen

2.7.2.4 Benutzerberechtigungskonzept: Rollen für das BW

Beim BW steht - wie ab dem Release 3.1G des R/3-Classic - der **Profilgenerator** (Transaktion PFCG) als Tool zur Automatisierung der Rechteerstellung zur Verfügung. Der grundlegende Begriff hierbei ist die **Rolle**, in älteren Releasesständen **Aktivitätsgruppe** genannt; die Zusammenfassung von Einzel- zu **Sammelrollen** ist möglich.

Analog zum Berechtigungsprofil werden durch die Rolle die Aktivitäten für die einzelnen Aufgaben bzw. für die wahrzunehmende Funktion zusammengefasst. Die benötigten Rechte werden automatisch (menügestützt) mit Hilfe des Profilgenerators erstellt.

Die Umsetzung der ermittelten Anforderungen erfolgt in den Teilschritten:

- Festlegung der benötigten Arbeitsplätze im Sinne einer unter Funktionstrennung gegliederten Aufgabenfestlegung für die jeweiligen Anwendergruppen
- Festlegung der benötigten Transaktionen und / oder Verwendung der seitens der SAP ausgelieferten Standardrollen je Arbeitsplatz
- Nacharbeit der automatisch vorgeschlagenen Berechtigungen

- Generieren der Profile und Berechtigungen
- Anlage/Pflege von Benutzerstammsätzen
- Test durch die Fachbereiche; ggf. Durchführung von Anpassungen
- Abschließende Freigabe durch den Fachbereich
- Transport der Rollen in das Produktivsystem

Zum Schutz personenbezogener Daten ist ein sachgerecht ausgestaltetes Berechtigungskonzept für die gesamte BW-Systemlandschaft und damit für Entwicklungs-, Qualitätssicherungs- und Produktivsysteme notwendig. Die jeweiligen Rollen sollten erst produktiv eingesetzt werden, nachdem das Test- und Abnahmeverfahren die Wirksamkeit der Zugriffsschutzmaßnahmen bestätigt hat.

SAP liefert neben Standardrollen auch nach wie vor Standardprofile (z.B. SAP_ALL oder SAP_NEW) aus. Aus Sicherheitsaspekten sollen diese nicht verwendet werden.

Verweis: *Leitfaden Datenschutz für SAP R/3*, Kapitel 4.2.4

Um die Aufgaben der Systembetreuung wahrzunehmen, sind ähnliche Rollen (u.a. Benutzerverwaltung, Systemüberwachung, Operating) wie beim R/3-Classic zu erstellen. Eine besondere Bedeutung erhält der Systembetreuer im BW-Umfeld, der die Richtigkeit und Vollständigkeit der Datenübernahme zu kontrollieren und ggf. notwendige Korrekturen zeitnah veranlassen muss.

SAP liefert rund 500 Standardrollen aus, zum einen zur Nutzung des BW, zum anderen für die BW-Administration. Diese sind derzeit sehr allgemein gehalten und müssen unternehmensspezifisch ergänzt werden.

Für das Reporting müssen nach Maßgabe der genutzten Informationen und Auswertungsanforderungen eigene Rollen aufgebaut werden.

2.7.2.5 Benutzerberechtigungskonzept: fachliche Ausgestaltung

Im Vergleich zu R/3-Classic-Systemen ergeben sich unter Datenschutzaspekten bei BW-Installationen besondere Risiken. Sie liegen

- in den Systemschnittstellen, da ein BW-System seine Daten aus vorgelagerten Systemen in einer bestimmten Periodizität bezieht (Eingabekontrolle),
- in den Transformationserfordernissen und Änderungsmöglichkeiten der personenbezogenen Daten im BW-System (Eingabekontrolle),
- in den besonderen Methoden der Datenhaltung und der Auswertungsmöglichkeiten (Zugriffskontrolle) und
- in dem Zusammenführen von Daten aus mehreren Quellsystemen wenn sich daraus im BW-System neue Reportingmöglichkeiten ergeben. Hier sind vorrangig Maßnahmen im Berechtigungskonzept erforderlich, um die zu unterschiedlichen Zwecken erhobenen Daten getrennt verarbeiten zu können.

Im Folgenden wird anhand eines Beispiels dargelegt, welche Arbeitsplätze über das Berechtigungskonzept differenziert werden können. Dabei ist hervorzuheben, das die zuzuweisenden

Rechte je Arbeitsplatz sich regelmäßig unterscheiden in Abhängigkeit davon, ob sie für ein Entwicklungs- / Qualitätssicherungs- oder Produktivsystem ausgestaltet werden. Ferner sind für die SAP-Quellsysteme Rollen auszuprägen, welche für den Datenexport zuständig sind. Werden SAP-fremde Quellsysteme eingesetzt, so sind auch in diesen Fällen für die Quellsysteme Zugriffsschutzmaßnahmen zu berücksichtigen.

Bei dem Arbeitsplatz „Anwender“ ist regelmäßig für ein differenziertes Reporting auf personenbezogene Daten eine deutliche Zergliederung nach Maßgabe der jeweiligen Aufgaben und Befugnisse notwendig.

Arbeitsplatz	Zuzuordnende Rechte (Beispiele)	Nicht zuzuordnende Rechte (Beispiele)
Anwender	Ausführen bestehender Berichte, wobei nach Maßgabe der spezifischen Reporting-Anforderungen die Arbeitsplätze zu differenzieren sind	Definition von Berichten Anlage / Pflege von Benutzern / Rollen
Entwickler Fachbereich	Definition von Berichten; ggf. Anlage / Pflege von Queries; ggf. Customizing (nur im Entwicklungssystem)	Systemadministration (insb. Transport von geänderten Objekten); Anlage / Pflege von Benutzern / Rollen
Entwickler IT	Customizing (nur im Entwicklungssystem); Verwaltung der Workbench	Systemadministration (insb. Transport von geänderten Objekten); Ausführen bestehender Berichte
Qualitätssicherung	Anzeige von InfoCubes; Prüfung der PSA (Persistent Staging Area)	Definition von Berichten Customizing
Basis- / System-Administration	Verwaltung der Workbench; Laden von Daten aus dem Quellsystem; Transport von Systemänderungen / Rollen	Customizing Definition von Berichten Anlage / Pflege von Benutzern / Rollen
Datenbank Administration	Pflege der Datenbankparameter	Definition von Berichten Anlage / Pflege von Benutzern / Rollen
Benutzer Administration	Anlage / Pflege von Benutzern	Definition von Berichten Anlage / Pflege von Rollen
Berechtigungs Administration	Pflege von Rollen (PFCG + RSSM)	Definition von Berichten Anlage / Pflege von Benutzern
Revision/Datenschutz	Anzeige von Benutzern; Nachvollzug wesentlicher Einstellungen / Sicherheitsparameter; Nachvollzug Transformationsregeln	Definition von Berichten Anlage / Pflege von Benutzern / Rollen

Arbeitsplatz	Zuzuordnende Rechte (Beispiele)	Nicht zuzuordnende Rechte (Beispiele)
ALE Remote (Hintergrundbenutzer)	Laden von Daten aus dem Quellsystem als Hintergrundbenutzer	Anlage / Pflege von Benutzern / Rollen
Notfall (Vergabe eingebunden in ein Notfallkonzept)	Sämtliche Zugriffsrechte	Keine

2.7.2.6 Besonderheiten bei der Berechtigungsprüfung

Im BW gelten bezogen auf das Ausschalten von Berechtigungsprüfungen (Transaktionen SU24 Berechtigungsobjektprüfung unter Transaktionen und SU25 / SU26 Upgradetool für den Profilgenerator), den Schutz von Programmcodes (Authority Check) sowie den Schutz von Reports über Berechtigungsgruppen / Zuordnung zu Transaktionen dieselben Regeln wie im R/3-Classic.

Es ist zu beachten, dass insbesondere auch die RSR-Objekte (eigenerstellte Objekte mittels RSSM) ebenfalls ausschaltbar sind.

Verweis: Die hierbei geltenden Fakten und Risiken finden sich in Kapitel 4.2.5. des *Leitfadens Datenschutz für SAP R/3*.

Zusätzlich sind bei Einsatz eines Portals weitergehende Maßnahmen bezüglich der Authentifizierung zu treffen und zu überwachen.

An dieser Stelle soll noch einmal darauf hingewiesen sein, dass durch eigenerstellte Berechtigungsobjekte erweiterte Schutzmöglichkeiten bestehen und die Umsetzung eines detaillierten Nachvollzugs bedarf.

2.7.2.7 Benutzer- und Berechtigungsadministration

Ganz allgemein ergeben sich keine Unterschiede zwischen der Benutzeradministration zwischen dem R/3-Classic und dem BW, so dass das bereits realisierte Verfahren - unter Verwendung des Profilgenerators - auch für das BW Gültigkeit erlangen kann.

Verweis: Kapitel 4.2.6 des *Leitfadens Datenschutz für SAP R/3*

Ergänzend zum Leitfaden stehen folgende vier Berechtigungsobjekte zur Verfügung, die eine Verwendung von Zertifikaten, die Möglichkeiten zum Ausschalten von Berechtigungsobjekten und den Einsatz der Zentralen Benutzerverwaltung steuern:

- Zertifikatsanmeldung, Zertifikatsanforderung und -zuordnung (S_USERCERT)
- Berechtigungswesen: Berechtigungsobjekte global ausschalten (S_USER_OBJ)
- Users: System specific assignment authorization objects (S_USER_SAS)
- Benutzerstammpflege: System für die zentrale Benutzerpflege (S_USER_SYS)

Zusätzlich ist bei der Rechte-Administration eine Rolle zur Verwendung der Transaktion RSSM zur Anlage von neuen Berechtigungsobjekten zu erstellen.

2.7.2.8 Änderungen am Produktivsystem

Zur Sicherstellung der Protokollierung von Änderungen sind dieselben Systemeinstellungen wie beim R/3-Classic vorzunehmen: Change and Transport System, Tabellenprotokollierung / Customizing, Systemänderbarkeit (Transaktion SE06), Protokolle (auf den entsprechenden Datenbanken), Tabelle T000.

Verweis: Kapitel 4.2.7 des *Leitfadens Datenschutz für SAP R/3*

Eine besondere Bedeutung kommen Datenänderungen im BW-Produktivsystem zu, da das BW primär als Auswertungstool zu verstehen ist (vgl. 2.8.2.9). Hierbei ist insbesondere der Funktionsbaustein RSAR_ODS_API_PUT zu nennen.

Möglichkeiten zur Änderung von übergebenen Originaldaten: Die übergebenen Daten werden zunächst in eine Persistent Storage Area (PSA) geladen und dann in die Datenziele (InfoCubes) fortgeschrieben. Die PSA-Daten sind zu Debugging-Zwecken für den Administrator einsehbar. Bei einer fehlerfreien Fortschreibung gibt es keine Möglichkeit, die Daten zu verändern.

Falls aber die Fortschreibung der Daten aus dem PSA in ein Datenziel nicht erfolgreich war, d.h. ein fehlerhafter Request z.B. durch unzulässige Werte in Form von Sonderzeichen vorliegt, können die PSA-Daten verändert und anschließend manuell fortgeschrieben werden. Da dieser Vorgang nicht protokolliert wird, sollte diese Änderungen entsprechend dokumentiert werden. Alternativ kann im Fehlerfall der Request komplett aus dem BW gelöscht und nach Beseitigung der Ursache erneut geladen werden.

Diese Möglichkeit ist aus Datenschutzgründen vorzuziehen, um eine Identität zwischen übergebenen und übernommenen Daten sicherzustellen.

Die prinzipielle Nutzung dieser Änderungsmöglichkeit ist durch BW-Berechtigungsobjekte geschützt (S_RS_ISOUR).

2.7.2.9 Systemschnittstellen

Für die Kommunikation zwischen einem BW und Fremdsystemen (SAP oder Non-SAP-Systeme) stehen ähnliche Möglichkeiten wie beim R/3-Classic zur Verfügung.

Verweis: Kapitel 4.2.8 des *Leitfadens Datenschutz für SAP R/3*

Nicht mehr benötigt wird das Batch-Input-Verfahren.

Innerhalb des BW kommt hingegen dem RFC (Remote Function Call) eine besondere Bedeutung zu, da die Daten aus dem Originalsystem mittels dieser Schnittstelle ins BW übertragen werden.

Auch weiterhin möglich ist der PC-Download, der mittels des Berechtigungsobjektes S_GUI unterbunden werden kann. Die Downloadmöglichkeit ist im Rahmen der unterschiedlichen Auswertungswerkzeuge (vgl. Kap 2.7) weiterhin differenzierter zu betrachten. Da die Anzeige im Rahmen des BEx Analysers grundsätzlich über MS EXCEL erfolgt, können die angezeigten Inhalte von jedem Benutzer auch auf ein lokales Medium gesichert werden. Dieser Vorgang kann nicht durch eine Berechtigungsprüfung abgefangen werden. Gleichermäßen verhält es sich, wenn der Benutzer über einen Web Browser auf die Daten des BW zugreifen kann. Lediglich im Falle der Nutzung des SAPGUIs greift der Schutz über das Berechtigungsobjekts S_GUI noch.

Empfehlung: Lassen Sie den Zugriff auf das BW mittels BEx Analyser und/oder Web Browser nur in den Fällen und für die Benutzer zu, in denen die Möglichkeit der Änderung des Auswertungszwecks datenschutzrechtlich unbedenklich ist oder wo durch andere technische, organisatorische und qualifikatorische Maßnahmen die Verarbeitung dieser Daten ausschließlich im Rahmen der vorhandenen Rechtsgrundlagen gewährleistet ist.

2.7.2.10 Auditing und Logging

Ganz allgemein ist das BW ein Auswertungstool, das nur die folgenden eingeschränkten Möglichkeiten zur Datenänderung vorsieht:

- Laden von Informationen aus dem vorgelagerten System
- Transformation
- Zugriffe auf die Tabellenebene.

Analog zum R/3-Classic sind die Konfiguration und Auswertung der Protokolle sowie manuelle Änderungen mit dem DSB abzustimmen.

Verweis: Kapitel 4.2.9 des *Leitfadens Datenschutz für SAP R/3*

Innerhalb des BW ist das AIS derzeit noch nicht verfügbar, da diese Komponente an das Vorhandensein der FI-Komponente geknüpft ist. Seitens der DSAG ist ein Entwicklungsantrag gestellt und von SAP anerkannt worden, den Teil „System Audit“ in die Basis-Komponente zu integrieren.

Keine Bedeutung innerhalb des BW hat die Report-Protokollierung innerhalb des HR. Dagegen müssen Änderungen an Systemeinstellungen analog dem R/3-Classic protokolliert werden. Hierzu stehen mit dem Security Audit Log, dem System Log und der Transaktionsprotokollierung STAD dieselben Möglichkeiten zur Verfügung.

Darüber hinaus ist die Protokollierung der Datenübernahme mittels Ladeprotokollen gegeben. Ein Nachvollzug dieser Protokolle ist mit der Transaktion RSMO möglich.

2.7.2.11 Zusammenhang Leitfäden Datenschutz R/3 - BW

Thema aus Leitfaden Datenschutz	Leitfaden BW
4.1 Anforderungen	2.7.1 Identisch, daher nur kurze Einführung
4.2.1. Identifizierung und Authentifizierung	2.7.2.1 Weitgehend identisch; Ergänzung um Beschreibung der Neuerungen hinsichtlich Anmeldung von Endbenutzern
4.2.2 Standardbenutzer	2.7.2.2 Identisch
4.2.3 Benutzerberechtigungskonzept: ausgewählte Berechtigungsobjekte	2.7.2.3 Komplett neu unter Nennung aller neuen BW-Berechtigungsobjekte sowie der Transaktion RSSM zum Erstellen eigener Objekte

Thema aus Leitfaden Datenschutz	Leitfaden BW
	2.7.2.3 Systemrechte sind ähnlich; es wird nur auf generelle Unterschiede hingewiesen
4.2.4 Benutzerberechtigungskonzept - ausgewählte Profile	2.7.2.4 Neu mit einer Beschreibung zum Profildenerator / Rollenkonzept 2.7.2.5 Neu: Beispiel für fachliche Ausgestaltung des Rollenkonzepts innerhalb von BW
4.2.5 Besonderheiten bei der Berechtigungsprüfung	2.7.2.6 Ähnlich; RSSM als neues Thema
4.2.6 Benutzeradministration	2.7.2.7 Ähnlich, Erweiterung um neue Berechtigungsobjekte für Benutzeradministration
4.2.7 Änderungen am Produktivsystem	2.7.2.8 Ähnlich; Beschreibung von Möglichkeiten der Datenänderungen innerhalb des BW
4.2.8 Systemschnittstellen	2.7.2.9 Ergänzung um Beschreibung der grundlegenden Unterschiede
4.2.9 Auditing und Logging	2.7.2.10 Beschreibung der Unterschiede (insb. kein AIS; Wichtigkeit der Ladeprotokolle)
4.2.10 Komplexe Suchhilfe	Kein relevantes BW-Thema
4.2.11 Zusammenfassung zentraler Risiken	3.1 Ähnlich; Ergänzung um Hinweise auf spezielle Risikofelder
4.3 Zusammenfassung der Prüfungshandlungen	3.2 Prüfungshandlungen wurden um BW-spezifische Prüfungen ergänzt

3 Risiken / Bewertung der Fallgruppen

Bei der Verarbeitung von personenbezogenen Daten in einem Data Warehouse werden besondere Risiken für die Persönlichkeitsrechte der Betroffenen gesehen. Diese sind namentlich:

- die Entkopplung der Datenbestände von den operativen Verarbeitungsverfahren und damit die Verselbständigung dieser Datenbestände.
- Die Möglichkeit zur Zusammenführung von Daten, die in den operativen Systemen getrennt verarbeitet werden;
- Die Gefahr der Zweckentfremdung der Daten;
- Die Verarbeitung außerhalb des rechtlich zulässigen Rahmens;
- eine vom Gesetzgeber nicht gewollte und von der Verfassung nicht erlaubte Vorratsspeicherung ohne Zweckbindung;
- im Rahmen der öffentlichen Verwaltung die Verletzung des grundrechtlich geschützten Verbots der Erfassung und Speicherung für unbestimmte Zwecke;
- eine Zweckänderung ohne Möglichkeit des Betroffenen zur Abschätzung der inhaltlichen und zeitlichen Tragweite der Einwilligung;
- Wirksamkeit der Einwilligung nach § 4a BDSG nur bei freier Entscheidung des Betroffenen (dies ist im Arbeitsverhältnis umstritten), Aufklärung über Zweck, Hinweis auf Konsequenzen der Verweigerung, in schriftlicher Form, wenn keine besonderen Umstände vorliegen. (Bei Data Warehouse Systemen weiß der Betroffene bei seiner Einwilligung meist nichts über die Zwecke und worauf er sich einlässt)
- eine Umgehung der Notwendigkeit, den Betroffenen von der Zweckänderung im Vorhinein in Kenntnis zu setzen;
- einen Verstoß gegen das Gebot der Datenvermeidung und der Datensparsamkeit (z.B. durch mangelnde Pseudonymisierung oder Anonymisierung, in beiden Fällen darf dem BW-Nutzer eine Identifizierung von Personen nicht möglich sein);
- eine Umgehung der gesetzlich vorgegebenen Speicherfristen
- durch die Wahl des Mittels BW faktische Unterlaufung der rechtlich zwingenden technisch-organisatorischen Maßnahmen;
- die Gefahr, dass durch ungeprüfte Übernahme von technischen Vorschlägen keine ausreichende Sicherstellung der rechtlichen Anforderungen möglich ist;
- die fehlende Kontrollierbarkeit die Absenkung des Schutzniveaus;
- eine Gefährdung der Datenschutzziele auf Grund der besonderen Komplexität der Datenverarbeitung in Business Warehouses

Diesen Risiken muss – neben der sorgfältigen Gestaltung der Business Warehouses – mit geeigneten technisch-organisatorischen Maßnahmen und Prüfungshandlungen entgegen gewirkt werden. Spezifische Prüfungshandlungen für BW finden sich in Kapitel 3.2. Allgemeine Prüfungshandlungen zu SAP R/3 Systemen sind ergänzend in Kapitel 4 des *Leitfadens Datenschutz für SAP R/3* zu finden.

3.1 Zusammenfassung zentraler Risiken

Generell bestehen beim BW-Einsatz weitgehend identische Risiken wie bei der Verwendung von R/3-Systemen. Daher kann auch an dieser Stelle auf den *Leitfaden Datenschutz für SAP R/3* (hier Kapitel 4.2.11) verwiesen werden.

Zusätzlich erwachsen besondere Risiken hinsichtlich der Zulässigkeit der Datenverarbeitung: Zum einen besteht das Risiko, dass die Daten nicht nur zu dem vereinbarten Zweck verarbeitet werden (Änderung der Transformationsregeln), zum anderen, dass mehr Einzeldaten als festgelegt an das BW übergeben werden (Erweiterung der Übergaberegeln).

3.2 Zusammenfassung der Prüfungshandlungen

Bei der Prüfung von BW-Systemen gelten grundsätzlich vergleichbare Prüfungshandlungen wie bei R/3-Systemen.

Verweis: Eine ausführliche Beschreibung zu den Prüfungshandlungen findet sich im Kapitel 4.3 des *Leitfadens Datenschutz für SAP R/3*. Im Folgenden werden Besonderheiten bezüglich BW-Systeme aufgeführt. Dabei wird an der bewährten Gliederung im *Leitfaden Datenschutz für SAP R/3* festgehalten, nämlich in die Abschnitte:

- Anforderungen an die Prüfbarkeit
- Gegebenenfalls gesonderte technisch-organisatorischen Anforderungen aus vorrangigen Rechtsvorschriften z.B. aus Betriebs- oder Dienstvereinbarungen
- Anforderungen der Datenschutzmaßnahmen gemäß § 9 BDSG und der Anlage

3.2.1 Anforderungen an die Prüfbarkeit

Hardware
Zusätzlich zu den unter 4.3.1.1 des im <i>Leitfaden Datenschutz für SAP R/3</i> aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:
<p>Welche Quellsysteme werden für das BW-System verwendet?</p> <p>Wie ist der Datentransfer von den Quellsystemen zu dem BW-System hardwaretechnisch realisiert?</p>
Betriebssystem und systemnahe Software
Zusätzlich zu den unter 4.3.1.2 des im <i>Leitfaden Datenschutz für SAP R/3</i> aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:
- keine-
Programmiertechnik
Zusätzlich zu den unter 4.3.1.3 des im <i>Leitfaden Datenschutz für SAP R/3</i> aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:
Programmentwicklung, Programmtests und Test von Customizing-Einstellungen

Existieren verbindliche Richtlinien bezüglich des Einsatzes und der Vorgehensweise bei den Programmier-Techniken ?

- Web Programmierung
- XML Programmierung
- ABAP Dictionary / ABAP Workbench
- Data Modeler
- Business Object Repository
- Kundenerweiterungen
- CATT-Testfälle (Computer Aided Test Tool)

Sind die Berechtigungen zur Programmierung in dem BW-Entwicklungs- und – Produktionssystem sachgerecht ausgestaltet und zugeordnet?

Nehmen Sie Auswertungen über die Transaktion SUIM zu den anwendungsbezogenen Berechtigungsobjekten (z.B. S_DEVELOP, S_TABU_DIS, S_TABU_CLI, S_TABU_LIN, S_TRANSPRT, S_CTS_ADMI) und zusätzlich zu dem Berechtigungsobjekt S_TCODE z.B. bezüglich folgender Transaktionen vor:

- RSA1 Administrator Workbench: Modellierung
- SD11 Data Modeler
- SE09 Transport Organizer
- SE11 Dictionary
- SE38 ABAP Editor
- SWO1 Business Object Builder
- SQ07 ABAP Query

Programmdokumentation

Werden Programme und eigenerstellte Objekte nachvollziehbar dokumentiert?

Neben den Transaktionen SA38 für die Überwachung der systemseitig hinterlegbaren Programmdokumentation und SE11 für die Tabellendokumentation stehen folgende Transaktionen zur Verfügung:

- SE80 Object Navigator
- SWO2 Business Object Browser
- SE95 Modification Browser

3.2.2 Prüfung spezieller Regelungen aus vorrangigen Rechtsvorschriften

Anhang zu Benutzerberechtigungen

Zusätzlich zu den unter 4.3.2 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Werden bei dem BW-System eigenerstellte BW-Berechtigungsobjekte verwendet? Prüfen Sie diese mit Hilfe der Transaktion SUIM und der Selektion auf mit „S_RSR“ und „Z“ beginnende Objekte.

Berücksichtigen die Übersichten über die zugriffsberechtigten Benutzer die Festlegungen aus den eigenerstellten Berechtigungsobjekten? Ist der SOLL- und IST-Stand der zugriffsberechtigten Benutzer abstimmbar? Verwenden Sie für die systemseitigen Prüfungen den Report RSUSR002.

Welche Quellsysteme werden für das BW-System verwendet?

Wie ist der Datentransfer von den Quellsystemen zu dem BW-System technisch und organisatorisch realisiert?

3.2.3 Prüfung der Datenschutzmaßnahmen gemäß § 9 BDSG und Anlage

Ziffer 1: Zutrittskontrolle

Keine gesonderten Maßnahmen für SAP BW-Systeme.

Ziffer 2: Zugangskontrolle

Zusätzlich zu den unter 4.3.3.2 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Wie ist der Zugang zu dem BW-System geregelt? Welche Verfahren (z.B. SAP Logon, Portal Excel-Plugin) werden verwendet und ist dabei eine hinreichend sichere Identifizierung der Benutzer sichergestellt?

Ziffer 3: Zugriffskontrolle

Zusätzlich zu den unter 4.3.3.3 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Werden eigenerstellte BW-Berechtigungsobjekte verwendet? Nehmen Sie hierzu Auswertungen mit Hilfe der Transaktion SUIM vor.

Sind diese eigenerstellten Objekte sachgerecht dokumentiert?

Wird über die korrespondierenden Rollen bzw. Berechtigungen ein angemessener Zugriffsschutz für personenbezogene Daten gewährleistet? Nehmen Sie Auswertungen mit Hilfe des Reports RSUSR002 vor.

Welche Benutzer besitzen die Möglichkeit, Daten unmittelbar aus der PSA (Persistent Staging Area) zu lesen bzw. dort zu manipulieren? Die PSA wird auf der Datenbank durch transparente Tabellen abgelegt. Werten Sie daher die zugriffsberechtigten Benutzer bezüglich folgender Berechtigungsobjekte aus:

- S_TABU_DIS – Tabellenpflege (insb. auch mandantenunabhängige Tabellen)

- S_TCODE – Transaktionscodeprüfung (z.B. bezüglich SE16, SE17, SQVI)

Analysieren Sie ferner die zugriffsberechtigten Benutzer in Bezug auf die folgenden Funktionsbausteine:

- RSSM_API_REQUEST_GET Verknüpfung von InfoSource und Requests
- RSAR_ODS_API_GET Datensätze der PSA-Tabelle lesen
- RSAR_ODS_API_PUT Geänderte Datensätze in die PSA-Tabelle schreiben

Sind die Zugriffsrechte in Bezug auf die Administration der InfoSources sachgerecht ausgestaltet und an die Benutzer vergeben? InfoSources stellen in der Regel die Grundlage für das Reporting dar. Prüfen Sie hierzu die Berechtigungen zu dem Berechtigungsobjekt

- S_RS_ISOUR Administrator Workbench – InfoSource.

Kritisch zu werten sind vor allem Ausprägungen zu der Aktivität mit dem Wert 03 (InfoSource-Daten anzeigen) und 23 (InfoSource-Übertragungsregeln / InfoSource-Daten pflegen).

Welche Benutzer besitzen die Möglichkeit, personenbezogene Daten in ODS-Objekten zu lesen bzw. dort zu manipulieren? ODS-Objekte (Operational Data-Store-Objekte) dienen zur Ablage von bereinigten Stamm- oder Bewegungsdaten. Auf der Datenbank werden die ODS-Objekte wie PSA-Daten durch transparente Tabellen repräsentiert. Prüfen Sie somit Anwendung und Umfang von ODS-Objekten sowie die zugriffsberechtigten Benutzer analog zu den Zugriffsrechten bezüglich der PSA.

Ziffer 4: Weitergabekontrolle

Zusätzlich zu den unter 4.3.3.4 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Wird eine Übersicht/Liste über diejenigen Stellen geführt, an die Datenübermittlungen programmgesteuert stattfinden können. Bei SAP BW sind dabei einerseits in das BW-System liefernde Systeme und andererseits aus dem BW-System belieferte Systeme zu berücksichtigen.

Ziffer 5: Eingabekontrolle

Zusätzlich zu den unter 4.3.3.5 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Die Ladeprotokolle sind insbesondere auf Einhaltung der betrieblichen Vereinbarung hin zu überprüfen (Transaktion RSMO).

Ziffer 6: Auftragskontrolle

Zusätzlich zu den unter 4.3.3.6 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Keine

Ziffer 7: Verfügbarkeitskontrolle

Zusätzlich zu den unter 4.3.3.7 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Keine

Ziffer 8: Gewährleistung der Zweckbindung

Zusätzlich zu den unter 4.3.3.8 des im *Leitfaden Datenschutz für SAP R/3* aufgeführten Aspekten sind folgende Prüfungshandlungen zu nennen:

Ist auf der Ebene des Zugriffsschutzes eine ausreichend strikte Zuordnung Benutzer/Funktionen/Befugnisse zu zulässigen Zwecken vorhanden? Prüfen Sie spezifisch für BW auch für Benutzer und einzelne Benutzergruppen die Zugänglichkeit

- Business Explorer Analyser (Transaktion RRMX)
- BEx Monitor / Query Monitor (Transaktion RSRT1)

4 Literaturverzeichnis

- Hornberger, Werner; Schneider, Jürgen: Sicherheit und Datenschutz mit SAP-Systemen, Kapitel 11, Data Warehouse und Datenschutz - ein Widerspruch? Galileo Press, Bonn 2000.
- Mehrwald, Christian: SAP Business Information Warehouse 3: Architektur, Konzeption, Implementierung. dpunkt-Verlag, Heidelberg 2003.
- Müller, Stefan, Product Management HR, SAP AG: HR im Business Information Warehouse
- Neumann, B., Eine komplette Reporting-Lösung für mySAP Business Intelligence, in: SAP INFO, 10.6.2003.
- Roßnagel/Scholz, Datenschutz durch Anonymität und Pseudonymität, in MMR 2000, S. 721 ff.
- Seemann, B.; Schmalzridt, P.; Lehmann: SAP Business Information Warehouse. Galileo Press, Bonn.
- SAP White Paper: mySAP Business Intelligence. In: Data Warehousing mit mySAP Business Intelligence, Version 1.1.
- SAP Business Information Warehouse, Functions in Detail. Version 1.0 SAP BW 3.0B. Product Management Business Intelligence, SAP AG.

5 Index

- Administration 38
- Administrator Workbench 8, 16, 17, 18, 19, 20, 21, 32, 35, 40, 48, 55, 56, 57, 58, 59, 62, 71, 72
- Aggregat 21, 57
- aggregierte Daten 8, 49
- Analysen 15, 67, 74
- Anonymisierung 10, 11, 37, 39, 41, 49, 69
- Archivierung 27, 41
- ASAP 24, 25, 28
- Aufbewahrungsfristen 32, 41
- Auftragsdatenverarbeitung 36
- Auswertungsmöglichkeiten 13, 26, 44, 46, 63
- BDSG 5
 - § 11 36
 - § 28 Abs. 1 14
 - § 3 11
 - § 3 Abs. 9 34
 - § 3a 11
 - § 4a 69
 - § 4b, 4c 36
 - § 4e 31
 - § 9 27, 34, 53, 70, 72
- Benutzerrollen 26, 27
- Benutzerverwaltung 63, 65
- Berechtigungskonzept 7, 10, 33, 34, 47, 62, 63
- Betriebsvereinbarung 10, 13
- Bewegungsdaten 8, 16, 18, 19, 20, 21, 40, 72
- Browser 15, 18, 44, 66, 67, 71
- Business Blueprint 25
- Business Content 22, 25, 28, 29, 35, 46, 47, 49, 50, 51, 52, 53
- Business Explorer 8, 42, 43, 44, 46, 55, 60, 61, 74
- BW Statistik 32, 33, 35
- BW-Administration 15, 63
- Customizing 27, 35, 64, 66, 70
- Data Mart Interface 33
- Data Warehouse 7, 9, 37, 69, 75
- Data Warehousing 7, 9, 38, 75
- DataSource 8, 16, 17, 21, 39, 40, 59
- Datenbasis 13, 48
- Datenformat 17
- Datenmodell 25
- Datenschutzbeauftragter 5, 25, 29, 32, 35, 39
- Datensparsamkeit 9, 11, 13, 27, 37, 69
- Datenübergabe 13
- Datenübernahme 25, 26, 37, 63, 67
- Datenvermeidung 9, 11, 13, 27, 37, 69
- Debugging-Tool 61
- Dienstleister 11, 36
- Download Scheduler 15, 46
- Drittland 36
- Einführungsmethoden 24
- Einwilligung 10, 14, 37, 69
- Empfänger 26, 31, 32, 33, 34
- EU-Datenschutz-Richtlinie 31
- EU-Richtlinie 5, 11, 37, 53
- Extraktionsstruktur 16, 17, 40
- Extraktor 16, 28
- Formatted Reporting 15
- Funktionsübertragung 36
- InfoCube 8, 20, 21, 44, 57, 62
- InfoObjects 8, 17, 18, 19, 20, 22, 28, 29, 32, 33, 39, 40, 45, 48, 62
- InfoPackages 21, 33
- InfoProvider 20, 32, 44, 60
- InfoSource 8, 17, 19, 20, 39, 40, 58, 59, 72
- Konvertierungsregeln 19
- Kundennamensraum 22
- Ladeprotokoll 34, 67, 68, 73
- Leitfaden Datenschutz für SAP R/3 5, 10, 25, 31, 32, 34, 36, 53, 54, 61, 63, 65, 66, 67, 69, 70, 72, 73, 74
- Logging 67, 68
- Löschungsfristen 27
- Metadata Repository 17, 18, 19, 20, 21, 32, 35, 36
- Metadaten 18, 28, 35, 36, 39, 56, 58, 59
- ODS-Objekt 13, 20
- Open Hub Service 33
- Operational Data Store
 - ODS 8, 19, 20
- Persistent Staging Area 8
- Personalplanung 37
- Persönlichkeitsrechte 9, 69
- Produktivbetrieb 27
- Projektplanung 29, 37
- Projektvorbereitung 25
- Prüfbarkeit 70
- Prüfungshandlungen 35, 68, 69, 70, 72, 73, 74
- PSA 8, 13, 17, 19, 39, 62, 64, 66, 72
- Pseudonymisierung 11, 13, 37, 39, 49, 69
- Quellsystem 15, 16, 17, 25, 32, 33, 64, 70, 72
- Query 23, 41, 48, 49, 60
- Query Designer 15, 41, 43
- Query Monitor 35, 74
- Rechtsgrundlage 10, 14, 26, 49
- RemoteCube 8
- S_GUI 66
- SAPGUI 15, 66
- sequentiellen Datei 8
- Sicherheitsleitfaden 5, 25, 27
- Solution Manager 24, 25, 28, 29
- Speicherungsdauer 10, 13
- Staging Area 17, 26, 64, 72
- Stammdaten 8, 17, 19, 20, 21, 40, 58, 61, 62
- Sternschema 8, 21
- Systembetreuung 63
- Tabellenprotokollierung 66
- technisch-organisatorische Maßnahmen 26, 32, 34, 53
- Transaktion
 - PFCG 55, 62, 64
 - RS02 17

Transaktion	STAD 67
RSA1 16, 32, 33, 35, 71	SU24 65
RSMO 35, 67, 73	SU25 65
RSRT 35	SU26 65
RSRT1 74	SUIM 33, 71, 72
RSRTRACE 61	SW01 71
RSSM 55, 61, 64, 65, 67, 68, 72	SWO2 71
SA38 71	Transferstruktur 16, 17, 19, 21, 40
SBIW 17	Transparenz 14, 31
SD11 71	Übermittlung 26, 27, 32
SE06 66	Übersichten 31
SE09 71	Übertragungsregeln 8, 19, 40, 58, 59, 72
SE11 71	Vorabkontrolle 11, 25, 31
SE16 62, 72	Vorratsspeicherung 10, 69
SE17 72	Web Application Designer 15, 43, 46, 61
SE38 62, 71	Zulässigkeitskriterium 10
SE80 71	Zusammenführung 8, 37, 69
SE95 71	Zweckänderung 10, 69
SM04 33	Zweckbestimmung 31, 37, 47
SPRO 17	Zweckbindung 8, 10, 14, 26, 53, 69, 74
SQ07 71	Zweckbindungsgebot 37
SQVI 72	

Glossar

In: <http://help.sap.com>

<http://www.sap-ag.de/germany/> → Suche

<http://www.sapinfo.net/public/de/glossary.php4>