

DSAG Work Group Revision Work Group Data Protection

Data Protection Guide for SAP BW

Release 3.1
Status 28th November 2003

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



SAP® AG • Neurtstr. 16 • D-69190 Walldorf
This document is subject to modifications and additions

Data Protection Guide for SAP BW

Foreword	5
0 Introduction	7
1 Legal Requirements for an SAP Business Warehouse (BW)	10
2 SAP Facts and Data Protection Aspects	15
2.1 Data Retrieval and Data Retention.....	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.....	19
2.1.5 InfoCube.....	20
2.1.5.1 Updating.....	20
2.1.5.2 Star Schema.....	21
2.1.5.3 Aggregate	21
2.1.6 Business Content.....	21
2 Implementation Methods	24
2.2.1 ASAP and Solution Manager	24
2.2.1.1 Project Preparation	24
2.2.1.2 Business Blueprint	25
2.2.1.3 Realization Phase	26
2.2.1.4 Production Preparation, or Final Preparation	26
2.2.1.5 Go Live and Support	27
2.2.1.6 Recommended Procedures	27
2.2.2 Business Content.....	27
2.3 Overviews	29
2.4 Contractual Data Processing	34
2.5 Data Transfer (De-Personalizing Data , Aliasing)	35
2.5.1 De-Personalization or Aliasing upon Transfer.....	35
2.5.2 De-Personalization upon Query Creation.....	39
2.5.3 Data Aging and Archiving	39
2.6 Views / Reports.....	40
2.6.1 Reporting Tools.....	40
2.6.2 Reporting Options	42
2.6.3 Access Rights with Self-Developed Reports.....	43
2.6.4 Business Content Reports.....	44
2.6.4.1 Examples from Non-HR Applications	46
2.6.4.2 Business Content for HR Data	47
2.7 Implementation of the Requirements from Section 9 BDSG and Appendix: Technical-Organizational Measures	51
2.7.1 Requirements	51
2.7.2 SAP-Facts, Risks and Measures.....	51
2.7.2.1 Identification and Authentication.....	51
2.7.2.2 Standard User	51
2.7.2.3 User Authorization Concept: Authorization Objects for BW.....	52
2.7.2.4 User Authorization Concept: Roles for the BW.....	59
2.7.2.5 User Authorization Concept: Effective Design	60
2.7.2.6 Special Features of Authorization Check	62
2.7.2.7 User and Authorization Administration	62
2.7.2.8 Changes to the Productive System	62

2.7.2.9 System Interfaces	63
2.7.2.10 Auditing und Logging	63
2.7.2.11 Correlation of Data Protection Guides for R/3 - BW	64
3 Risks / Evaluation of Case Groups	66
3.1 Summary of Main Risks.....	67
3.2 Summary of Audit Activities	67
3.2.1 Requirements for Auditability.....	67
3.2.2 Checking Special Regulations from Overriding Regulations.....	69
3.2.3 Checking the data protection measures according to section 9 BDSG and appendix	69
4 References	72
5 Index.....	73
Glossary	74

Foreword

This guide is targeted at data protection officials for SAP users and consultants. It describes requirements compliant with data protection legislation as well as technical facts on the SAP Business Information Warehouse (SAP BW Rel. 3.1 Content) and provides details about risks, their evaluations and the associated audit activities.

It supplements the SAP security guide and the *Data Protection Guide for SAP R/3* and like these, it is only to be considered a recommendation. The responsibility for compliance with the data protection provisions remains with the companies and their data protection officials. This guide is based on the EU Directive 95/46/EC and the German Federal Data Protection Act (BDSG) 2001¹ as to data protection legislation.

This guide was composed by members of the work group Data Protection in the DSAG Work Group Revision/Risk Management, who would like to share their experiences. Most of the authors were also involved in the creation of *Data Protection Guide for SAP-R/3* Release 4.6.

© Copyright 2003 of the authors:

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

The authors are responsible for the content. Editorial post-editing is done by SAP AG, Walldorf.

Note: This document is copyrighted. No part of this text may be reproduced in any form without prior permission from the authors. Any usage of this text in form of duplication, translation, microfilming, feed-in and processing in electronic systems is prohibited.

The authors of the **Data Protection Guide** would appreciate your input, suggested changes or additions. This is true for suggesting enhancements of individual chapters as well as for providing examples from concrete test experience.

In order to make it easier for you to reply, you will find a response form on the following page:

¹ as of 14th January 2003

To the spokesperson for the
Data Protection Work Group
c/o Mr. T. Barthel
FORBIT/CArO
Eimsbüttelerstr. 18
D-22769 Hamburg
E-mail: barthel@forbit.de

FAX: +49-40/4398296

Sender: Name:
Function:
Department:
Company:
Address:
.....
Phone: Fax:

Subject: Additional Information about the *Data Protection Guide for SAP BW*

I refer to

SAP Data Protection Guide BW, chapter:.....
SAP BW system, Release:

My comments:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

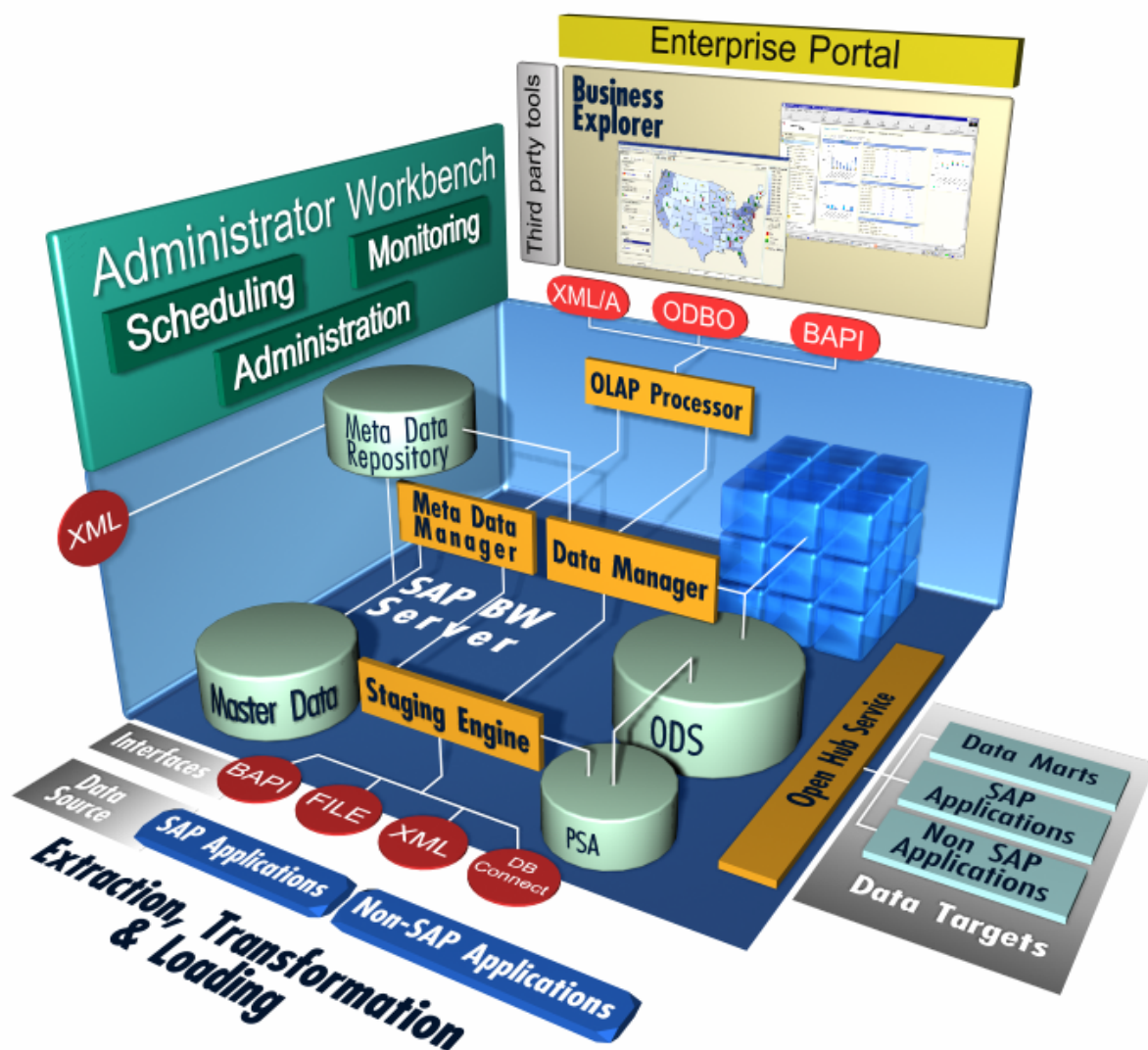
I have included more information on a separate sheet (Please check):

Yes No

0 Introduction

Nowadays, in order to make effective decisions, companies need precise and up-to-date information from all different sources, such as marketing, production, sales and distribution, finance and human resources. This information is stored in various application systems and data sets within and outside the affiliated group. The concept for the integration and consolidation of this data is called ‚Data Warehousing‘.

‚Data Warehousing‘ is an independent application environment with an associated database that is supplied with data from various sources and that facilitates flexible queries and analyses. The Data Warehouse system offered by SAP is called the SAP Business Information Warehouse (SAP BW).



The basis of the SAP BW is an R/3 kernel with the known authorization concept that has been enhanced by several authorization objects to control the rights for extraction, administration and data access and by a front-end tool for report access. As mentioned above, one of the requirements of a Data Warehouse system is the possibility of grouping data from a number of different platforms. Therefore, there are interfaces to SAP R/3, R/2 and BW systems as well as to non-SAP systems in SAP BW. Sequential files may also be imported.

The data in the source systems that logically belongs together is called the **DataSource**. In the first step, it is transferred into an inbound storage area, the (**PSA** = Persistent Staging Area), where it is saved unchanged in relational database tables. With transfer rules, it is then determined how these fields are to be grouped together as InfoObjects and InfoSources.

InfoObjects are the smallest units in BW. They structure the business evaluation objects, such as customers, sales and so on. They are divided into characteristics, units and time characteristics to describe the type of values (for example the sales with third parties in million €in 2002) and key figures (= values) such as quantities, amounts or number of items.

An **InfoSource** is a quantity of InfoObjects for a type of business event that logically belong together. An InfoSource can contain either transaction data or master data from one or several source systems.

The data is subsequently updated in ODS objects or InfoCubes for long-term storage.

ODS objects (**O**perational **D**ata **S**tore) provide a long-term data storage location for consolidated and cleaned-up transaction data on the document level from one or several InfoSources. They are stored in transparent flat database tables, such as the PSA .

From a reporting point of view, an **InfoCube** describes a self-contained dataset that is the central object for multidimensional reports and analyses in BW. It provides an aggregated data storage that is optimized for reading in order to enable performant, multidimensional analyses. Basic InfoCubes are supplied with data from one or several InfoSources or ODS objects. They generally store aggregated data in a number of relational tables according to the star schema (multiple dimensions). However, if the transaction data is not managed in BW, it is a RemoteCube. The data is only available during the runtime of a report on the RemoteCube in BW.

For further details on information objects in BW see chapter 2.1.

The Administrator Workbench is a tool for managing data and processes. With the help of the Administrator Workbench, all processes connected with data staging and processing can be controlled and monitored. Besides it provides an overview of all existing information objects in BW.

The Business Explorer (BEx) is another tool for analyzing the data. It is a reporting and analysis interface with predefined standard reports and freely definable lists. In addition, third-party tools can also be used.

Generally, the basic question that arises first is whether and in what form the processing of personal data should be allowed in a BW. There are a number of data protection experts who believe that this is in principle legally problematic.

For example, due to data aggregation, for example with statistical methods, it is possible to 'dig out' new relations and to create personal profiles without much effort. In addition, due to comprehensive data collection, new insights into the entire relation, for example, the affiliated group, are provided. The joining of data may be critical as well. So the intended purpose of use, for example, will not be kept to in all cases.

On the other hand, the prerequisite for effective Data Warehousing is global use of data within the company, for which the same "depth of focus" as in conventional data sets is not required. Therefore, the chance arises here to take appropriate measures to promote the principle of data reduction and data economy and to completely avoid any personal reference as often as possible.

This means that Data Warehouse systems basically increase interference with personality rights, but on the other hand, they may also improve the protection of such rights. With the following statements, we wish to limit the risks and to strengthen the protection.

1 Legal Requirements for an SAP Business Warehouse (BW)

Data privacy law prohibits the acquisition, processing and use of personal data and allows data processing only in compliance with the prerequisites defined in the data privacy laws (prohibited without express permission). Therefore, processing of personal data is only possible with an appropriate legal foundation, which essentially consists of the consent, works agreement and stipulations.

According to the data privacy law, preliminary data is used in Business Warehouse (BW) and except for the creation of analyses, all other data processing occurs in the preliminary operational systems.

This also means that the legitimacy of acquiring and processing data generally has to be clarified ahead of time within the context of the operational systems. The information contained in the *Data Protection Guide for SAP R/3* should be considered for the SAP systems used there.

For the BW system, we need to specifically clarify to what extent the processing of the collected data is still needed for the original purposes. The BW is often used in the individual interest of the company, irrespective of the original legalities regarding permission, for example, privity of contract (change of purpose). In this context, it has to be considered that, with the discontinuation of limitation of use for specific purposes, there is a case of illegal data retention. This especially applies if data is at first only being collected in the BW system and the analyses are to be specified at a later date.

In a lot of cases, access to personal data is not required. The SAP BW is used to optimize the operational process chains without the need for evaluating personal data.

If the BW system is only used to support the operational system, the data protection officials for the company can restrict testing to the authorization concept. The prerequisite is that the purpose, data range, storage time and group of people with access authorization not be extended.

Except for the above-mentioned systems that are, for example, only placed behind a R/3 system to enable easier analyses with reporting tools, the collection of personal data from homogeneous systems should be evaluated legally in a different way due to the limitation of use for specific purposes.

In addition to creating new legalities regarding permission, for example by consent from the affected party, “de-personalizing” remains as an eligibility criterion. If all personal data is uniquely rendered anonymous, which means that it is impossible to identify individuals, the data protection provisions are no longer applicable.

In case of “aliasing”², however, the data protection act is still applicable, since, although the data is initially anonymous to the viewers, the reference to individuals can be re-established at any time. In this context, the decisive aspect here is who owns the assignment table and is thus able to restore the direct reference to individuals³.

In all cases, the data protection official should be consulted well before the implementation of a BW system in order to clarify the complex data protection facts of the case. Even prior checking might be necessary.

For the evaluation of the BW system it also has to be clarified as to whether personal data or anonymous or aliased data is transferred to the BW and which of these three data classes are kept in readiness in the basis or evaluated by the InfoCubes (see example of a BW HR system in figure 1). Further requirements might become necessary if the BW or the upstreamed systems are used by a supplier (see figure 2).

² EU Directive

Recital 26

The principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.

Article 6

(1) Member States shall provide that personal data must be:

c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; ...

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

BDSG

Section 3 BDSG, Further definitions

(6) “Rendering anonymous” means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual

(6a) “Aliasing” means replacing a person’s name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult.

§ 3a BDSG, data reduction and data economy

Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection.

Directive 95/46/EG of the European Parliament and the Council from 24th October 1995 for the protection of individuals with regard to the processing of personal data and for free movement of data calls for data reduction and data economy.

³ This opinion is currently being discussed since the aliasing is according to the BDSG (§ 3a BDSG) the recommended means for data reduction and data economy. On the other hand, according to the wording of the BDSG this does currently not imply an easier processing.

Recently people like Rosnagel/ Scholz⁴ or the committee of experts „Modernisation of the data protection law, especially basic amendment of the German Federal Data Protection Act“ have spoken out against it. They rightly aim at whether the assignment with the concrete processing is possible and intended. If this is not the case, for example, if the assignment table 5 is kept under lock and key by another department, the data are anonymous to the user with the above-mentioned consequences.

Figure 1:

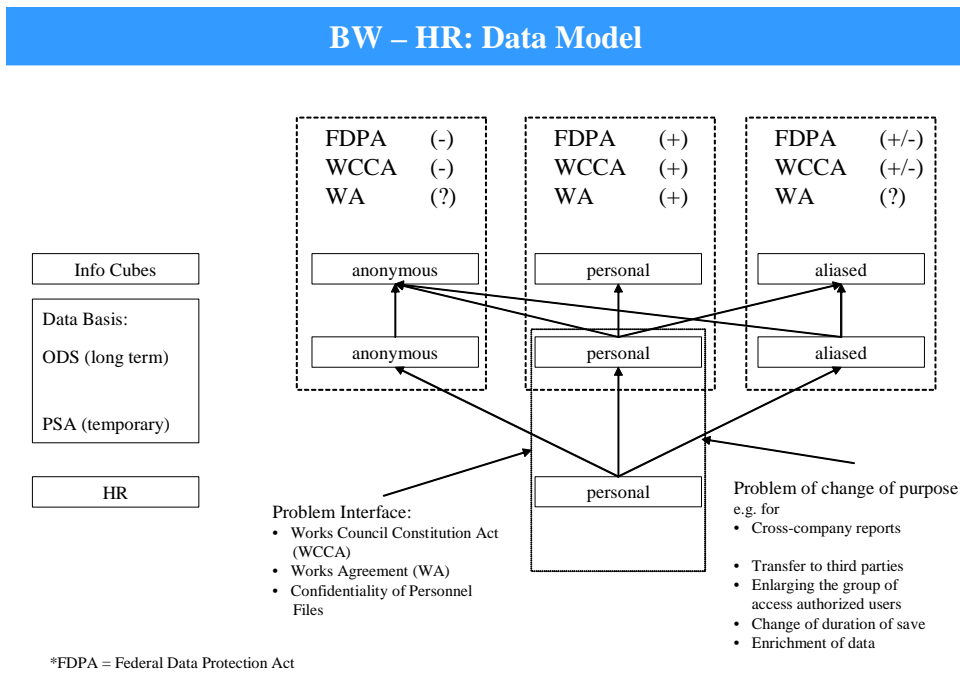
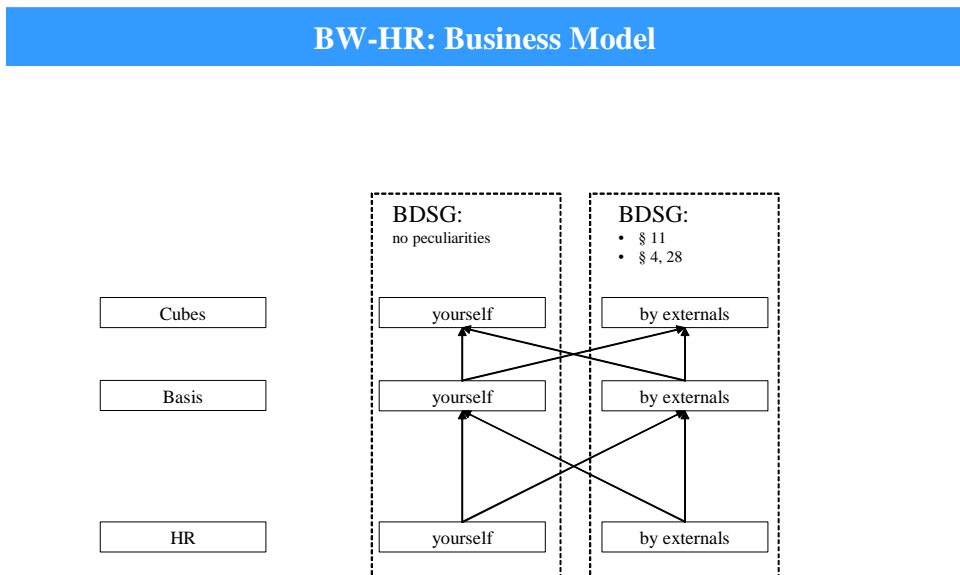


Figure 2:



Checking areas:

This means that there are basically the following three checking areas:

- a) Data transfer to BW
- b) Keeping data in the basis
- c) Type and range of views and analyses provided by the InfoCubes

to a) data transfer to BW

- Even if only data rendered anonymous is transferred to the BW and the data protection law is neither applicable here nor to the handling of this data, you need to check whether the existing works agreements or specific legal provisions regularize the anonymous transmission and use.
- If personal or aliased data are to be transferred to the BW, it has be checked beforehand as to whether there are
 - o Provisions (special obligations to maintain secrecy, for example professional secrecy, confidentiality of personnel files or secrecy of telecommunications, banking or tax secrecy) or
 - o Existing works agreements in the area of personal data processing or
 - o Data protection provisions

that restrict or even prohibit the transfer.

Such a check is especially necessary if the BW system is not used to support the operational system, but if, for example the

- o purposes,
- o data range,
- o storage time,
- o the possibilities of analysis or
- o the group of persons authorized to access with the appropriate authorizations
- o are enhanced.

to b) Keeping data ready in the basis

The data basis is to be divided into PSA and ODS Object (see chapter 0).

The PSA basically serves to temporarily save the data transferred into the BW before it is stored in the final BW data basis (ODS Object).

This means that technical/organizational measures should specifically be observed with regard to the PSA and the principle of data reduction and data economy with regard to temporary storage. Generally, this means that the data are to be deleted in the PSA after a successful upload into the ODS objects.

With the ODS objects, the duration of storage should be considered in view of the business purpose and the related requirements. The requirements arise from the BW purposes. In this context, the scope of the saved data should be checked regularly.

to c) Type and scope of views and analyses provided by the InfoCubes

The following basic principles for data protection are the focus of the check:

- Limitation of use for specific purposes
- Clarification of the scope of the legal foundation from the operational systems for BW
- Creation of new legal foundations, for example by consent or contractual provisions (see Section 28 (1) BDSG)
- Transparency of data processing

Quality (data integrity and consistency)

2 SAP Facts and Data Protection Aspects

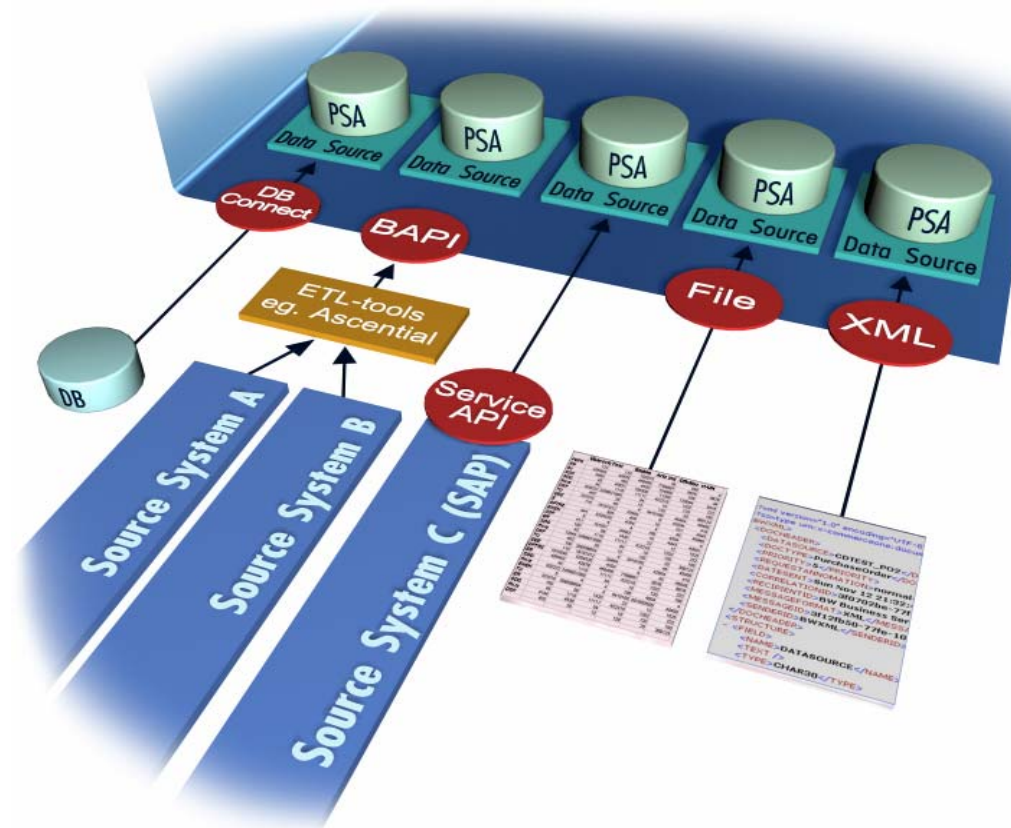
In contrast to a pure R/3 system, the end users do not log on to the Business Warehouse directly. Instead, they receive the required access using a portal or a front-end tool to execute or change reports. The logon via the SAPGUI that is familiar from R/3 is only necessary for BW administration, but it can also be done by an end user.

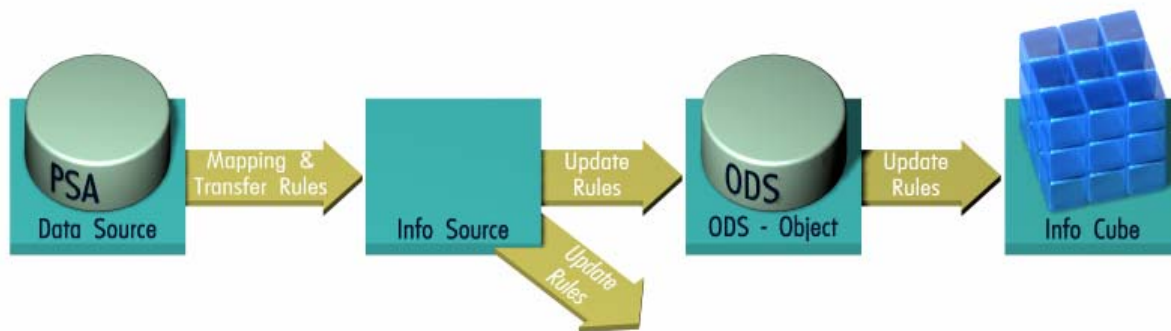
When the SAP front-end tools are installed, the Analyzer, browser, Download Scheduler, formatted reporting, Query Designer and Web Application Designer are installed. The authorization check is done in the BW system. If users have the proper authorization, not only do users have read authorization, they also have the option of changing reports.

2.1 Data Retrieval and Data Retention

The SAP BW System receives data from one or multiple operative systems. These can be either SAP (R/3, CRM etc.)- or non-SAP systems. In general these systems are designated as source systems.

In SAP BW, the data uploaded from the source systems is brought into a format that is meaningful for the company, that is, it is processed into information. The following graphics illustrate the data flow.





In the Administrator Workbench for the SAP BW system there are numerous functions that help provide an extensive overview of the source systems used and the objects defined in SAP BW.

If the tester needs to make a more detailed analysis of the overall data structure including the data flow, there are tools for this purpose in the Administrator Workbench (Transaction RSA1). Because extensive rights are necessary for this transaction (for example, change authorization), testing can only be done in cooperation with administration.

To obtain a list of the source systems used in the navigation menu for the Administrator Workbench, click on the „Modeling“ selection button. Then select the entry „Source systems“.

Menu path:

BW Administration -> Administrator Workbench -> Modeling -> Source systems

2.1.1 DataSource

The data supply of a source system in SAP BW is subdivided into contained business areas by DataSources. These areas are source-system dependent DataSource-types that are used for the transfer of master and transaction data. We differentiate here between two field structures:

- Extraction structure
- Transfer structure

The extract structure of a DataSource contains the amount of fields for the source system that is being offered for the data load process. The transfer structure represents a selection of fields for the extract structure of a source system. Using a special program called the extractor, the contents of the fields in the extract structure are transferred to the transfer structure. This is used to transfer the data from the source system to SAP BW.

To determine the DataSources for a specific source system, first click on the „Modeling“ selection button in the navigation menu. Then select the entry „source systems“. When you double click on the name of the sources system, the DataSources defined for this source system are listed in the display area of the Administrator Workbench.

Menu path:

BW Administration -> Administrator Workbench -> Modeling

When checking the SAP BW system, it can also be helpful to determine the extraction structure of a DataSource, that means to determine which fields from a source system are being provided to SAP BW. To do this, in the navigation menu, select the „modellierung“ entry and then click on „source systems“. Now, with the right mouse button, select the DataSource to be examined in the display area and click on “object overview” in the pop-up window that appears. An overview of the fields provided by a DataSource is then displayed in a new window, along with the names of the InfoObjects to which the data from these fields will be transferred.

In the source system (as long as it is an R/3 system), this information can be determined using the function „ Processing Generic DataSources “ (transaction RSO2) or „Subsequent Processing of DataSources“ (Transaction SBIW).

Transaction:

SPRO -> Press SAP Reference IMG button

Menu path:

Integration with Other SAP Components -> Data Transfer to the Business Information Warehouse -> Generic DataSource or Subsequent Processing of DataSources

You can get a list of all DataSources by selecting the „Metadata Repository“ in the navigation menu. Then select the entry „DataSource / FileSource“ in the display area.

Menu path:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.1.1 Persistent Staging Area

The Persistent Staging Area (PSA) is the initial store for data from source systems in SAP BW. The required data is saved there unchanged from the source system.

The data is saved in relational database tables (PSA tables) from SAP BW, the structure of which corresponds to the transfer structure; they also contain additional system fields. When there are changes to the transfer structure, a new version of the PSA table is created. The previous data format thus remains unchanged, which means there are no aggregations or transformations.

The data saved in the PSA tables can also be modified . The PSA proves to be another useful check, above all for assurance of data quality and for a correct data load process.

Before transfer into the InfoSource, you have the option of temporarily saving the transaction and master data in the PSA . This means the PSA can optionally be used as temporary storage for operational data. However, it is intended to be only a temporary storage (for a short time) and not to be used for permanent storage of data.

Menu path:

BW Administration -> Administrator Workbench -> Modeling -> PSA

2.1.1.2 Metadata Repository

A description of the source data (master- and transaction data) is created using the metadata (for example origin, history, and other aspects of the data). SAP BW recognizes three classes of metadata:

- Technical data
- User data and
- Business data (company definitions).

Technical metadata describe technical properties such as field length and data type. User metadata contains information about authorization. Company definitions provide SAP BW with the necessary comprehension of the business terminology. For example, special key performance indicators are defined here.

SAP BW is equipped with a central **Metadata Repository** which aids integrated, consistent and correct metadata and enables the reuse of metadata throughout the company. With the metadata repository, all SAP BW meta objects and the links between them are managed. The metadata **repository browser** provides the administrator with quick access to the metadata for all SAP BW objects.

You can search through the metadata repository according to technical names, descriptive texts and so on. Also, metadata can be swapped between various systems, HTML pages can be exported, and graphics can be displayed for the objects.

Menu path:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.2 InfoObjects

The smallest information modules (= fields) of SAP BW are designated as InfoObjects. They can be uniquely identified by their technical names. They are business evaluation objects that can contain data on cost centers, employees, customers, sales and so on.

InfoObjects have three main functions:

As a component of the metadata repository, they contain the technical information for the master- and transaction data in SAP BW. They are used throughout the system to build tables and structures with which the information can be displayed in SAP BW in a structure format. They are also used to define reports to analyze master and transaction data.

InfoObjects are classified by categories, that is, according to the type of data that they represent, such as characteristics and key figures. A characteristic could be, for example, a product, customer type, fiscal year, time period or region that is used to create report groups for an analysis. Key figures can be values or amounts such as sales revenues, fixed costs, sales quantity or headcount.

The functions of the Administrator Workbench provide you with a technical description of the InfoObjects. Here you should select „Modeling“ in the navigation area. The InfoObjects are listed and sorted according to InfoAreas in the display area. By double clicking on the desired InfoObject you get to the detail display for the InfoObject.

Menu Path:

BW Administration -> Administrator Workbench -> Modeling -> InfoObjects After selecting the „Metadata Repository” in the navigation menu and then clicking on the entry „InfoObject“, a list of the activated InfoObjects is displayed.

A list of InfoObjects sorted according to area can also be obtained by selecting the entry “InfoObjectCatalog”. Menu Path:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.3 InfoSource

An InfoSource is a quantity of InfoObjects that contain all the available information for a business process (e.g. cost center accounting). The structure in which this information is stored is called the **Communication Structure**. It is the technical realization of the InfoSource. Unlike the transfer structure, the communication structure is independent of the source system because it can be supplied from various source systems.

The InfoSource enables cross-system transport of data between source systems and SAP BW. Data requests for the source system are made by InfoSource and source system. InfoSources, like the underlying InfoObjects, can supply either transaction data or Master Data (Attributes, Texts and Hierarchies), whereas the structure of InfoSources for transaction and master data is almost identical.

After the source system data has been stored in the PSA, it can be directly loaded into the data store (Operational Data Store) or directly into the InfoCubes. This usually only occurs if there is no need to clean, transform or consolidate, that is for the preparation of the data transferred from the source system.

In general, the data received in SAP BW is prepared using **Conversion Rules/Transfer Rules** and transferred to the communication structure. The transfer rules determine which fields of the transfer structure are to be transferred into which fields of the communication structure or which fields are to be assigned to the associated InfoObjects of an InfoSource. Conversion rules are necessary if data is to be transferred into the necessary business logic during actions such as date/time conversions, character string operations and so on.

The data in SAP BW is then made available for further use using the communication structure.

Menu Paths:

BW Administration -> Administrator Workbench -> Modeling -> InfoSource

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.4 Operational Data Store

The Operational Data Store (ODS) is used to query granular data that is frequently updated. An Operational Data Store object (ODS object) is used to store consolidated and cleaned data (for example transaction data or master data) on the document level (basic level). It describes a consolidated dataset from one or more InfoSources.

The ODS object data is saved in transparent database tables. They can be updated using a delta update in InfoCubes or other ODS objects.

Info Objects, ODS objects and InfoCubes are also listed in SAP BW under the superordinate term „InfoProvider“. The ODS objects can thus also be found in the navigation menu by selecting „modeling“/„InfoProvider“. InfoProviders also include InfoSets, RemoteCubes and MultiProviders.

Menu Path:

BW Administration -> Administrator Workbench -> Modeling -> InfoProvider

You can display and further analyze the ODS objects by selecting the „Metadata Repository“ and then clicking on the entry „ODS object“ in the display area.

Menu Path:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.5 InfoCube

InfoCubes are the central objects of the multidimensional data model (data cube) in SAP BW. They contain a quantity of InfoObjects that logically belong together.

From a Reporting viewpoint, an InfoCube describes a closed dataset for a business area. The dataset represented by this (transaction data is exclusively saved in InfoCubes) can be evaluated using various front-end tools from various business perspectives, such as geographic region or type of distribution channel.

When creating a multidimensional InfoCube, update rules are created that are always defined using a combination of InfoCube and InfoSource. Hence, an InfoSource can update multiple InfoCubes; however it is also possible that an InfoCube be connected to several InfoSources.

You find both InfoCubes and ODS objects under the superordinate term „InfoProvider“. In the navigation menu, choose „Modeling“ and then the entry „InfoProvider“.

Menu Path:

BW Administration -> Administrator Workbench -> Modeling -> InfoProvider

You can display and further analyze the InfoCubes through the „Metadata Repository“. In the display area of the Metadata Repository, click on the entry „InfoCube“.

Menu Path:

BW Administration -> Administrator Workbench -> Metadata Repository

2.1.5.1 Updating

SAP BW supports two types of updates in which data can be loaded into SAP BW. The full update always extracts all data for the fields of a transfer structure. The second type of update is the delta update, which only extracts data that has changed since the last load process or that is new. Delta updates are especially suited to large data masses so that data does not have to be loaded into SAP-BW multiple times. Using InfoPackages, specific subsets of the data defined in the DataSource can be described. Using precise selection parameters (selection criteria, DataSource parameters, update modes and planning specifications), you define which transaction data or master data (for example, only controlling area 001 in period 10.2000“) of a DataSource is requested.

You can obtain a list of all defined update rules using the „Metadata Repository“. Select the „Update Rules“ entry in the display area by clicking on it with the mouse.

Menu path:

BW Administration -> Administrator Workbench -> Metadata Repository

You can display the update rules for InfoObjects, InfoCubes and ODS objects by selecting the respective object. To do this, follow the directions in this chapter.

2.1.5.2 Star Schema

When an InfoCube is created, the characteristics are summarized in dimension tables and are positioned around a central fact table that contains key figures. This schema is called a star schema. It classifies two groups of data: facts (for example, sales and quantity) and dimension attributes (for example, customer, material, and time). The facts are the focus of the analysis of corporate activity.

SAP BW works with an enhanced star schema in which master data (via attributes, hierarchies and texts) can be saved in separate tables that are used by all of the InfoCubes.

2.1.5.3 Aggregate

To reduce the data volume per query it is possible to implement aggregates. An aggregate is a materialized, aggregated view of the data or subsets of data for an InfoCubes. In an aggregate, the dataset for an InfoCube is saved redundantly and persistently in the database in compressed form.

Like database indexes, aggregates also improve performance, without the end user interfering with these processes or needing to have knowledge about their execution.

Aggregates can be created for:

- Characteristics
- Attributes and
- Hierarchies.

2.1.6 Business Content

The Business Content is delivered with SAP BW. The content includes a rich collection of preconfigured information models. This includes extractors, several thousand InfoObjects and several hundred InfoCubes and ODS objects. These also have predefined templates for reports and analyses with all of the associated technical and business definitions for Business Content. Some of these objects are branch specific; some are area or function-specific, for example for Customer Relationship Management and Supply Chain Management. Another part of this concept is the so-called technical content (for example, information models), with which the administrator can determine how individual objects can be used in SAP BW.

The Business Content, provides the company with a starting point for data modeling and analysis. As needed, the company can: install the Business Content without changes, create

new content, or customize Business-Content objects to suit its own specific requirements. In many cases, the latter is more efficient than creating a completely new object. To help you differentiate between the individual InfoObjects and SAP-delivered objects, SAP InfoObjects start with 0 and the customer's InfoObjects start with the letters A to Z.

Customer Namespace

To avoid name conflicts with the customer's local objects, the customer content has to be developed in its own namespace. You can either use your own namespace (apply for one with SAP) or an agreed upon subarea of the standard customer namespace (A* to Z*).

SAP Namespace Table

	SAP Namespace	Example	Table in the ABAP Dictionary
InfoObjects	0xx_	0ME_CITY01 City Name	
		0MATERIAL	/BI0/PMATERIAL
InfoObjects	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 two-character abbreviation for the IBU

0xxx_ wo xxx three-character abbreviations for the software components

Industry Solutions

Abbreviations	Industry Business Unit (IBU)
AD	Aerospace and Defense
AF	Apparel and Footwear 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
OI	Oil & Gas
PH	Pharmaceuticals
PU	Public Sector
RT	Retail
SP	Service Provider
TE	Telecommunications
TA	Transportation
UC	Utility Companies

Example: A special attribute of *Retail Materials Management* requires the following InfoObject:
ORT_MAT

Software Components (Examples)

Abbreviation	Software Components
APO	Advanced Planner and Optimizer
MSA	Mobile Sales
CRM	Customer Relation Management

Abbreviation	Software Components
SEM	Strategic Enterprise Management
EBP	Enterprise Buyer (Procurement)
FRE	Forecast & Replenishment Engine
MAP	Merchandising & Assortment Planning
RPA	PIPE (PointOfSales Inbound Processing Engine)

Example: A special attribute of *Mobile Sales* requires the following InfoObject **0MSA_CUST**.

2 Implementation Methods

Basically, there are two different ways of implementing a BW. One is the classic implementation method using procedure models with ASAP, now called Solution Manager. The second is the procedure that involves examining and changing templates – called Business Content in regard to BW.

2.2.1 ASAP and Solution Manager

In the past, SAP recommendations for implementing the Business Information Warehouse followed the general ASAP model for mySAP components. In the future, the Solution Manager will replace the ASAP model. In addition to the general procedure model, the ASAP model or the Solution Manager contains special accelerators for BW. The following chapter mainly deals with the activities in the procedure model that have a relationship to the requirements of data protection. The corporate/regulatory data protection official, in dealing with the Business Information Warehouse to be implemented, should especially focus on these tasks and as needed, he should adapt the aspects that are relevant for concrete implementation in the project/subproject. If a preliminary check is necessary, these points have to be examined individually before the BW system goes live.

The ASAP procedure model generally differs in the following five main phases: Project preparation (1), Business Blueprint (2), Realization (3), Production Preparation or Final Preparation (4) and GO-LIVE and Support (5). The focus of the data protection officer's dealings with the BW implementation project is undoubtedly on the Business Blueprint and Realization phases. The following will answer the main questions regarding data protection in the individual phases:

2.2.1.1 Project Preparation

Within the framework of *Project Preparation* we need to clarify how the data protection official is to be included in the project. This can include roles such as membership in the steering committee, a consulting function in project management or working actively in the individual project groups. No matter what the precise position in the project is and the extent

of the personal data in BW, the data protection work group recommends that the data protection official be a member of the SAP BW projects. Then, even if it is decided at the end of the project that no personal data is to be saved in BW, our experience has shown that there is quite a need for advice on the question of how personal data from the source systems can be kept out, that is made anonymous, aliased or aggregated and how they can prevent restoration of personal data.

In order to be able to appraise this, data protection officials must have a certain knowledge base regarding the technology available from SAP and its area of application. This can be obtained from reading the documentation (see <http://help.sap.com>), the Security Guide, the general *Data Protection Guide for SAP R/3* and in certain circumstances, by taking specific training courses at SAP AG or other institutions.

2.2.1.2 Business Blueprint

During the *Business Blueprint* phase, the data model has to be designed, the details of data transfer from the source systems to SAP BW need to be established, reports and reporting options have to be planned, user roles and authorizations have to be developed, and a plan for user training and documentation must be drafted.

On the one hand, the basic decisions need to be made within the framework of the data model and data transfer: Is there personal data in BW? If yes, can this data be de-personalized, aggregated or aliased? If yes, then where – in the source system or in the target system, in the initial area or when forming the InfoCubes? If the project requires storage of personal data in BW, then certain follow-up activities absolutely have to be discussed to fulfill the data protection requirements, such as:

- Is there a legal foundation for processing of personal data in BW?
- If the BW is operated in another company that is legally separate – such as the corporate group – which legal foundation exist for the transfer of data and for which purposes the recipient may process the data; what restrictions will there be on reporting and the use of reporting tools from the legal foundation?
- Is there the option of working with data that is de-personalized or aliased and still being able to assign the data records (perhaps using classification keys stored in encrypted form in the Staging Area, by forming Info Cubes with aggregated data, etc.),
- Which reporting methods and formats are permissible under the auspices of limitation of use of data processing?
- In which form should the overviews be delivered (for more information, see section 2.3 below),
- Which technical-organizational measures – especially in access rights – are required, etc.

Furthermore, during planning of reporting and reporting methods legal deliberations need to be made in regard to checking the legal foundation for saving, processing and deleting, as well as transferring data if access to the BW data is to be permitted for outsiders – such as corporate controllers. Here one also needs to check whether the missing legal foundation can be replaced with a newly created legal foundation in contracts and agreements. With cross-border data access, special attention should be paid to the regulations in chapter IV of the EU Directive 95/46/EC Article 25f. and its implementation in national law.

Finally, the requirements for user roles and the associated authorizations should be comprised. For the training and documentation steps, the future user's knowledge of data protection laws should be expanded and the existing need for information in this required should be maintained.

2.2.1.3 Realization Phase

During the *Realization Phase*, the requirements determined in the previous phases should be implemented using system settings and any further necessary programming. Any further changes that are required should be implemented and tested. The data protection official is then given the task of attending to implementation according to the requirements and to provide project consultation as needed. The following data protection activities are especially important in this phase:

- Organizational changes (for example, questions regarding responsibilities, etc.)
- Planning of training and documentation activities (including the question as to whether more extensive training of future users is necessary in the interest of data protection? If yes, with which content and in which form),
- Development of user roles and setting up authorizations (technical-organizational measures under the terms of Article 17 of the EU Directive, or according to the current nationally valid regulations such as section 9 BDSG), as well as
- Development of the assignment process for new authorizations and users (also within the above-mentioned technical-organizational measures);
- Customizing, especially mask design (according to articles 7 and 8 of the EU Directives, so that only the person who is processing the data sees only the data that is within his or her legal task requirements to fulfill);
- Development and tests of reporting and workflows;
- Configuration of the data extraction from the source systems (to implement the principle of data economy and data reduction especially when the source system and the BW are assigned to different legal entities, which means that data transfer takes place in the legal sense);
- Design of the data flow;
- Archiving (especially to check the storage period and deletion terms) and
- Test and acceptance of the settings;

2.2.1.4 Production Preparation, or Final Preparation

During production preparation, from a data protection point of view, copying over and testing functions should be performed using real data, training of end users should be accomplished and the effectiveness of the technical-organizational security mechanism should be checked. Lastly, especially compare the SAP recommendations in the Security Guide with special emphasis on quality assurance, consult the checklists in part 3 of the Security Guide .

2.2.1.5 Go Live and Support

For incorporation of productive operation, data protection layer quality assurance measures should be planned that constantly check the status of data protection measures in a continuous process and help with improvements. Experience has shown that, in projects of this size, in the introductory phase, and also during release changes, issues were overlooked that were only discovered during later checks and that could be improved upon.

2.2.1.6 Recommended Procedures

Follow the current ASAP/Solution Manager Implementation Guide. In the schedule, identify the steps you consider relevant and accelerators (both are part of the documents). Go through the pertinent documents with the project manager, discuss the data-protection relevant requirements and agree on project results over the course of the project. For this purpose, request a report on the current project status and begin discussions about the pertinent topics.

2.2.2 Business Content

Business Content is preconfigured roles and tasks and task-oriented information models in the SAP Business Information Warehouse based on consistent metadata. The Business Content provides the company with all of the objects so that employees can quickly build reports – from data extraction to roles that provide a company's employees with all the information they need to fulfil their tasks. The predefined Business Content helps to drastically decrease implementation time, independent of whether this content (as established by SAP) is integrated or serves as a starting point for creating customer-specific models.

These information models generally include roles, workbooks, queries, InfoSources, InfoCubes, ODS objects, key figures, characteristics, update rules and extractors for SAP R/3, mySAP.com Business Applications and other selected applications.

Business Content can:

- be used without the need for adjustment
- be adapted, that is honed to suit the user's needs
- be used as a template or example for customer-defined Business Content

Beyond that, the SAP Business Information Warehouse Demo provides content that includes example data and can be used as illustrative material.

Under collective term "Business Content", the SAP Business Information Warehouse provides preconfigured objects. These objects accelerate the implementation of the SAP Business Information Warehouse because they provide complete solutions for business information requirements.

Business Content includes:

- R/3 Extractor programs
- DataSources
- Process chains
- InfoObjects

- InfoSources
- Data targets (InfoCubes and ODS objects)
- Variables
- Data Mining models
- Queries
- Workbooks
- Crystal Reports
- Web Templates
- Roles

The implementation procedures by means of analysis and changing templates in the Business Content generally includes the following data-protection relevant steps:

- Project start with definition of project targets and project steps
- Project planning
- Forming project groups
- Training project members
- Setting up access to a system with Business Content
- Creation of a business blueprint for changes to the various objects, especially
 - o Changing the inbound data (DataSources)
 - o Changing the data models (InfoObjects, InfoSources, InfoCubes and ODS Objects)
 - o Changing views (Forming MultiCubes, queries)
 - o Changing authorization checks
 - o Changing the display of evaluations for the end user
- Changes in view of the available tools
- Creation and test of a authorization concept
- Implementation of changes
- Test of changes
- Productive activation

There is no formalized procedure – like when using using the Solution Manager – for changing the Business Content. The concrete procedure in the projects thus greatly depends on the degree to which the business requirements are fulfilled by the Business Content.

If a project for implementing BW using the BC is now “started”, the corporate/regulatory data protection official (and, in many cases, also the employee representative based on codetermination, e.g. sixth sentence of section 87 (1)) should be brought in early on.

Continuative starting points, where personal data is being processed in the Business Content, can be found in relation to the prepared reports in chapter 2.7.

2.3 Overviews⁴

To discern their tasks, data protection officials also receive documentation required by section 4e und 4g part 2 BDSG (see *Data Protection Guide for SAP R/3*, chap. 2.3).

The EU Data Protection Directive defines the minimum scope of the specifications in article 19 – **Contents of the Notification:**

(1) Member States shall specify the information to be given in the notification. It should include at least:

b) The purpose(s) of the processing;

c) A description of the category or categories of the affected persons and of the data or data categories relating to them;

d) The recipients or categories of recipients to whom the data might be disclosed;

e) Proposed transfers of data to third countries;

f) A general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

(2) The Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Purpose of the Overviews is to enable the data protection official to understand his tasks

- in checking the permissibility of processing personal data
- in preliminary checking and
- in instructing and training users
- to notify and provide information for those affected,

to allow the supervisory authority to check the implementation of data protection regulations and to create transparency of data processing for everyone.

In the *Data Protection Guide for SAP R/3*, Release 4.6, section 2.3 (Creating and Maintaining Overviews) provides extensive information about the format of the documentation, the public log register and the internal process directory in connection to the SAP R/3-System. These specifications are referred to expressly.

SAP BW systems are generally operated in addition to R/3 systems in order to simplify the process of referring back to overviews that have been completed there. However this is not sufficient in every case. Even if there is a 1-1 transfer (mirroring) to an operative SAP R/3 application, particular technical-organizational endeavors are required in order to reproduce the authorization structures for reporting with company-specific authorization objects (compare this to specifications in sections 2.7 and 2.8).

Normally **overview enhancements are necessary for SAP BW**, because

⁴ Overview is used in the sense of the list stipulated in the first sentence of Section 4g of the Federal Data Protection act, which includes information on automated processing procedures.

- the reason for processing for BW, in the sense of section 4e (4), is often not the same as the reasons for processing in the source system and are therefore not covered by the same legal foundations,
- the recipient or categories of recipient often exceed those of the source system (example: cross-company BWs),
- the period for retaining records and standard period of deletions are defined in the BW according to different principles than in the source systems,
- transmissions to third countries (in cross-company BWs) can also be managed differently than in source systems,
- in any case, the BW requires independent technical-organizational measures for saving the data that is saved and evaluated there (for example, company-specific authorization objects for reporting).

The **form of overviews for a SAP BW** with personal data may correspond to the form of other directories of proceedings that are also required (compare with the *Data Protection Guide for SAP R/3*, chapter 2.3.9). Remember, however, that all reasons for processing are to be listed before new processes are implemented. Where additional reasons that exceed the “old“ reasons for processing are determined subsequently, directories are to be updated before processing. The data protection official must have the opportunity to appraise the proceedings (on the basis of the updated directory) before personal data is processed.

For documentation on **determining reasons for data collection, processing and use**, see comments made in 2.3.2 in the *Data Protection Guide for SAP R/3*.

The **groups of persons affected and the data or data categories that relate to them** can be described in SAP BW by referring back to data in elementary modules in the BW. These are the InfoObjects or InfoSources that facilitate the data transport from source systems.

The BW Metadata Repository also delivers additional information on the data structures. (Compare to chapter 2.1).

BW statistics can also be used for this. Call the Administrator Workbench (transaction RSA1) and choose the *Modeling* area. Choose the InfoProvider tree. There, under the *Technical Content* InfoArea, you find the InfoArea *BW Statistics*, under which all InfoProviders for BW statistics can be found.

This is an analysis tool that is contained in the technical content of BW and allows you, for example, an overview of the usage of InfoObjects, InfoSources, source systems and queries (- > technical description in section 2.4). The following questions can be answered with BW statistics:

- Which InfoCubes, InfoSources, queries, aggregates are used in the system?
By comparing the SAP delivery version (D version) with the active version (A version) you are able to check which objects are used. In order to be able to work with objects they have to be transferred to the active version (A version).
- Which data is transported from where to where?
 - o Which data is currently being used in InfoCubes, InfoObjects, InfoSources, source systems, queries, and aggregates in the system?

Using the technical content (BW statistics) you can find out which departments or users have used the BW over a particular period of time (for example in the last quarter; in the last year).

The best way to check InfoSources and source systems is with transaction RSA1.

- Which datasets are moved?

This information is generated when InfoPackages are executed.

- Which users are working in the system?

With transaction SM04 you can display a user list, as you can in R/3

- Data output

If an existing Business Information Warehouse has already been defined as a source system, data mart interface functionality is used.

If you want to define an already existing Business Information Warehouse as a source system, use the data mart interface functionality. The data mart interface can be implemented between two BW systems or between an APO system (Advanced Planner and Optimizer) and a BW system.

The open hub service makes it possible to distribute data from an SAP BW system into non-SAP data marts and other applications. In this way, the controlled distribution into more than one system is guaranteed.

A description of the **recipient or categories of recipient** whose personal data can be communicated within the context of SAP BW can be obtained, if necessary, from the communication structures of the InfoSource or using the authorization concept (see chapter 2.8).

Persons or groups of persons for whom access is authorized.

With info system authorizations (transactions SUIM), those reports on users and authorizations that are available in the R/3 system are also available in BW.

Example of an overview including SAP BW

In the following example, reference is made to the *Data Protection Guide for SAP R/3* (chapter 2.3.9).

Public Part

Purposes of data collection, processing or use

mySAP BW: Definition and provision of key figures based on aggregated data for the personnel administration, the decentralized control of organization, recruitment, personnel management (payment, benefit, pension scheme), strategic personnel planning and personnel cost planning)

Groups of data subjects and the associated data or categories of data

Persons: Employees, applicants, customers, vendors, policy holders

Data: Data from employees, applicants, customers, vendors or policyholders from mySAP HR, mySAP FI and mySAP CRM

Special categories of personal data according to Section 3 (9) of the Federal Data Protection Act (BDSG) (Section 8 EU-RL), for example: operational health protection data or data for protection of labor from accident reports

Recipient or categories of recipients

Order data processors, group-related companies, especially holdings

Standard periods for the erasure of data

Periodical erasure after expiry of a preservation period, for example a preservation period of 3 years

Creating aggregated data records every third year

Planned data transfer in third states

Example: Parent company in Japan; sales companies in Central America, USA and Australia

Non-public Part

General description for assessing the adequacy of the data protection measures according to Section 9 of the Federal Data Protection Act (BDSG)

- Submission of a security concept on a separate form
- Planned log analyses: Security Audit Log, Syslog
- System environment: System software (operating system, DB, network), application software (mySAP BW)

Technical and organizational measures according to Section 9 of the Federal Data Protection Act (BDSG):

Control: Data protection official (DPO)

Access: Gate keeper, key

Access: PC log, password rules

Access: Authorization concept and protection of programs from modifications by the user

Transmission: see: access authorizations

Input: Change documents in the source systems; partly through the BW loading logs

Order: contractual provisions and sampling procedures by revision and by the DPO

Accessibility: DB recovery, back-up copies outside

Separation: Separation by roles/authorizations; no download permitted

Tasks and Authorizations of the DPO

In order to evaluate the set up of SAP BW regarding data protection or to perform the required audit activities, sufficient training of the data protection official in the use of the relevant SAP BW functions is necessary. The DPO should also have the required access rights in SAP BW.

On the recommendation of the data protection work group, SAP will develop a standard role for the data protection official, for example, SAP_Auditor_BW. This role has to be modified to fit operational requirements.

Until this is delivered, SAP recommends that data protection officials in enterprises using this function, issue (with read authorization) the role:

Z_ AUDITOR_BW (*naming suggestion*)

With this, the following functions can be accessed:

- BW statistics MultiProvider or queries
- Basis display profile S_A.SHOW (plus the authorization for displaying authorization management change documents and minus the authorization for displaying application data⁵)
- Administrator Workbench (RSA1): Authorization is to be restricted in the authorizations object S_RS_* to “display“ and sub object ”definition“.
- Monitor Administrator Workbench (RSMO)
- Query Monitor RSRT

The last three transactions may also have write authorization. In this case you will need the assistance of the administrator.

Technology for creating overviews for SAP BW

BW Metadata Repository:

With the HTML-based BW Metadata Repository you can access information on BW metadata from a central point. You can also access the most important object properties and their relationships to other objects. This enables you to find metadata, swap metadata, export HTML pages, and display graphic representations of objects.

Features:

In the Metadata Repository you can display both the active objects in the system (activated objects) and the SAP delivery objects in the system (Business Content). The object types existing in that particular system are listed in the window on the right-hand side of the screen. Hyperlinks make it possible for you to get a list of all objects for each object type. You can navigate to the information on the individual object from this object list.

Searching in the Metadata Repository:

⁵ Display options should be restricted to Customizing and system tables in authorization object S_TABU_DIS.

In this process, the technical name, the short and long texts, and the SAP documentation delivered on the objects available in the Metadata Repository are searched through.

HTML export:

Both active objects and SAP delivery objects can be exported as HTML pages. These can be made available to the data protection official.

Graphics:

Using XML-based vector graphic formats, metadata can be displayed for documents. It can be displayed on the Internet as VML graphics and SVG graphics.

2.4 Contractual Data Processing

When activating a service provider for operating BW, you have to take note of the prerequisites for function transfer and for contractual data processing . The principles involved here are referred to in chapter 5 in the *Data Protection Guide for SAP R/3*.

As far as service provider behavior is concerned, take note of the following cases:

Case 1:

The entire system (operative system and BW) is operated by a service provider. Here the service contract should only to be enhanced by the BW service fields.

Case 2:

One or more components only (operative system, basis of BW or InfoCubes) are operated by a service provider, and not the entire system.

When you use a service provider, a processing of order data with reference to data protection provisions is normally available for the services executed by the service provider. Independently of the basic admissibility check (see chapter 1), the prerequisites listed in section 11 of the Federal Data Protection Act are to be observed, see chapter 5 in the *Data Protection Guide for SAP R/3*.

Special case: Function transfer:

If the BW operator alone deals with the data (for example, cross-company reporting on company group), this normally requires a prior transfer of data. If there is no order data processing, provisions for data transfer have to be used, see chapter 5 in the *Data Protection Guide for SAP R/3*.

Special case: Third country:

When obtaining personal data in the context of operating a BW in a country outside of the EU or EEA, specific requirements for a so-called third-country transfer have to be observed with regard to attaining a suitable level of data protection (Federal Data Protection Act sections 4b, 4c, article 25, 26 EU-RL, see chapters 2.3.6 and 5.2.9 in the *Data Protection Guide for SAP R/3*). This is in addition to the normal admissibility prerequisites for operating a BW (see chapter 1).

In order to allow access to data from third countries, a separate BW system can be useful. After depersonalizing the appropriate data or aliasing it can be transferred to this separate BW system.

2.5 Data Transfer (De-Personalizing Data , Aliasing)

By merging data from different systems the aim is to obtain a unified and consistent view of customers, business processes and other aspects of business events. The merging of data in this way is often problematic because of indispensable data protection imperatives on the limitations of use. Personal data can only be accessed for a unique, determined and legitimate purpose. Data cannot be processed further in a way that is not compatible with the original purpose defined.⁶

The only criteria under which this is permitted are often the consent of the persons affected or the de-personalization or aliasing of the data. If you de-personalize data it can no longer be traced back to the individual and is therefore no longer subject to the strict terms of the Federal Data Protection Act.

A data warehouse is relatively static and normally designed for retrieving large amounts of historic data. In contrast to operative decision-making support, a data warehouse is used for strategic decision making.

Therefore you should make use of the fact that in many cases it is not actually necessary to access personal data in the BW system in order to obtain global insights. At the start of a project the question should not be which data can be extracted from the operative systems, but rather what information users require in order to cope with the challenges posed on a daily basis within an enterprise. For group-wide personnel planning, for example, you require aggregated information on headcount, movement of personnel, and employee structure, but personal details about individual employees such as age, gender, nationality, skills, or training remain in the BW feeder systems and can be viewed from that system by an authorized person in a subsequent detailed analysis.

Overviews at cost center level are often sufficient and a *drilldown* to the individual is not necessary.

This offers data protection officials the possibility of complying with the requirements of data reduction and data economy. The data protection official should use the opportunity to get involved in the project during the planning phase and to discuss the option of rendering data anonymous or pseudoanonymous upon data transfer. The data protection official, along with the workers representative, can check whether any personal reference is necessary. In this way, the danger of any potential performance assessment can be avoided.

2.5.1 De-Personalization or Aliasing upon Transfer

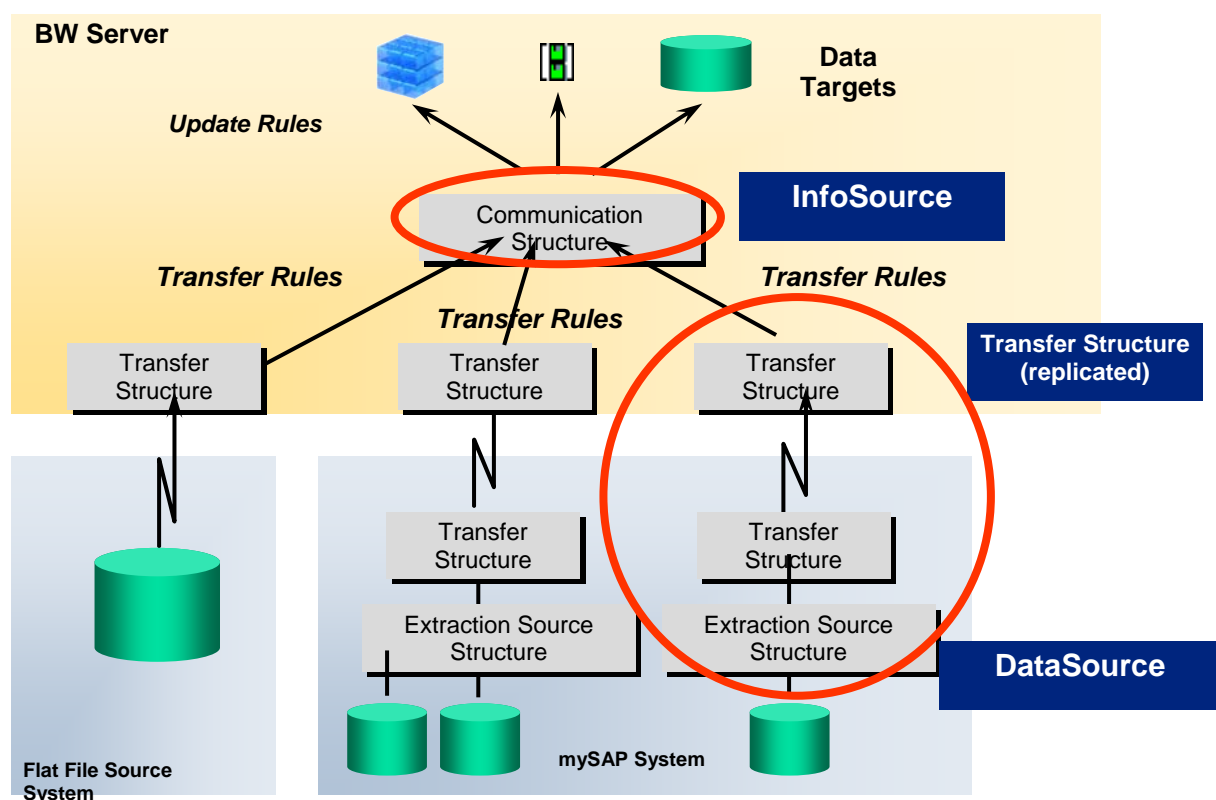
For reasons of data economy, only data that is absolutely necessary may be copied from the source systems. According to data protection principles, data has to be factually correct and up-to-date. You must first check whether it is possible to render particular fields anonymous

⁶ Article 6, EU Directives

in the source system or in a copy. Appropriate programs are available on the market for HR too⁷. However, the value of the data in BW must not be compromised by this.

Upon data transfer, you have to check which personal data has to be transported into the BW system. It is possible that you may have to extract more data from the source system than is actually needed for reporting. Data can be retained in ODS objects and InfoCubes and never displayed for the end user if it is required for building information units. Here you should note that this data may be accessible to certain privileged users such as the administrators, or that it may be the target of an attack if the SAP BW does not have the same high security status as the original personnel or customer system.

What options does SAP BW offer?



SAP Technology: Extract, Transform and Load

So that the data transferred is meaningful it must be integrated, standardized and consistent. This is ensured by the ETL process (Extract, Transform and Load).

⁷ Companies like BKC in Munster, Inside GmbH in Oldenburg (<http://www.inside-net.de/>), PECASO in Heidelberg (www.pecaso.com -> Clone&Test) or SQS in Cologne (http://www.sqs.de/solutions/solu_saptest.htm -> Test Suite for SAP R/3) offer programs of this sort.

ETL is a challenging element of data warehousing. Not only must the correct data sources be identified, but the value and admissibility of the data also have to be evaluated. The data protection official should also check the admissibility of the data at this point.

Extraction

Data extraction takes place either at application level or at database or file level (the “technical” level).

At application level, data is extracted in the form of business objects. One business object is usually displayed in several tables. The relations between the tables are defined by the application logic.

SAP applications in particular can be seamlessly integrated into SAP BW. Using data extractors, special extractors can be used for special objects in the source system (for example, for “Order” in mySAP CRM). Deltas can also be transferred from the source systems with extractors so that complete transfers can be avoided. Here users themselves determine how regularly data should be updated.

The staging BAPI (Business Application Programming Interface) allows data to be transferred from non-SAP sources. This is of particular importance for companies that favor internally developed extraction programs.

Extraction at database and file level requires that the data and corresponding metadata is called directly from the various tables. This form of extraction is suitable if the data is stored in “flat” files, if it is being sent using XML, or if it is saved in databases of old applications.

SAP BW offers comprehensive ETL functionality that facilitates data extraction at both application and database and file level.

The source data is saved in a PSA object (persistent staging area object), a transparent database table, in a physically unchanged form. The PSA is the initial store for data in the SAP BW information models. A PSA is generated for each DataSource and each source system.

Transformation

The next logical step is the movement of data from the DataSource to the InfoSource. This contains InfoObjects that are grouped together logically from the point of view of the enterprise. Data is cleaned up according to the transformation rules being used and is converted into information.

SAP BW offers a comprehensive library of transformation rules with which the appropriate business logic is assigned to data upon date/time conversions, character string operations, aggregation etc. If you want to avoid having to produce your own code, these transfer rules can be linked easily by using formulas from a transformation toolbox. During the assignment process it is determined exactly which data from the DataSource will be transferred to the InfoSource.

Implementation

In the control installation of the transfer it is also possible to systematically render data anonymous or pseudoanonymous. For example, the customer name, location and street can be simply overwritten or replaced.

Example:

The data transferred from a source system is partitioned into business-specific areas by DataSources. DataSources represent source system-dependent DataSource types that are used for transferring master and transaction data. The data is transferred to SAP BW with a two-dimensional or “flat” structure (that is as tables and not as a multidimensional data structure). The definition of the source data can be found in the DataSource.

Two different field structures can be distinguished: The **extraction structure** and **transfer structure**. The extraction structure contains all of the source system fields which are provided by so-called extractors. Extractors are programs that collect data from source systems. During extraction the content of the fields is transferred to the transfer structure.

The transfer structure represents a selection of fields from the extraction structure of the source system.

When data is uploaded it is transferred on a 1:1 basis from the transfer structure of the source system into the transfer structure of the SAP BW and then transferred to the communication structure of the SAP BW using transfer rules). Transfer rules serve to transfer data from the DataSource to the InfoSource and, where necessary, to transform and modify it. Using these transfer rules, the DataSource fields can be assigned to InfoObjects, which make up InfoSources. A comprehensive library with transformation functions is available for this purpose. These represent business logic.

InfoSources can contain both transaction data and master data. With transaction data transactions that are performed in an OLTP system (Online Transaction Processing), such as SAP R/3, are traced. These can be “quantified“ and can be of a high level granularity. Master data is the data that remains the same over a long period of time, such as customer addresses or the organizational structure of a company.

When you maintain transfer rules you determine whether the communication structure is filled with fields from the transfer structure, with fixed values, or by local conversion routines.

Conversion routines are ABAP programs which you can create yourself. Routines only ever refer to one InfoObject in the transfer structure.

You get to the maintenance of the transfer structure via the InfoSource tree in the Administrator Workbench. You can jump to the maintenance function from the context menu of a source system belonging to an InfoSource using the *Maintain Transfer Rules* function.

Various methods of transfer are possible:

- Data is transferred on a 1:1 basis (no manipulation of data)
- The communication structure fields can be filled with constants
- Transfer rules can be created on a flexible basis using local ABAP routines.

It is possible to encrypt data using the SSF (Secure Store Forward) interface. This can be connected using ABAP routines. It is also possible to de-personalize all of the data or alias it with an ABAP routine.

2.5.2 De-Personalization upon Query Creation

Query design enables you to quickly create and supply graphic and highly interactive analysis applications and reports. The Query Designer in mySAP BI defines how the user is able to analyze data, which information can be displayed (authorization) and which form of interaction is possible (navigation). Parameterization allows you to personalize queries in such a way that a query can be used by several users.

When creating queries it is also possible to exclude InfoObjects that should not be displayed. However, using the authorization concept it is also possible to create your query and implement restrictions later when you execute it. That means you can hide particular columns or only allow drilldown to a certain level. You are able to determine particular settings by using hierarchies.

2.5.3 Data Aging and Archiving

With a sophisticated data warehousing concept a data aging strategy is also necessary.

This is not just a matter of reducing costs (storage and performance), but also of taking into account the length of time for which data is retained before it is deleted. Data must not be allowed to accumulate limitlessly. Older data that is accessed rarely can still be necessary for analysis purposes. However you should also keep the volume of data necessary to a minimum for data protection reasons. You should also use the opportunity to remove any personal references that still exist from old data.

InfoCubes and ODS objects can be converted into archive files with the Archiving Development Kit (ADK). They can then be saved using third-part archiving technologies, for example, in visual and hierarchical memory management systems.

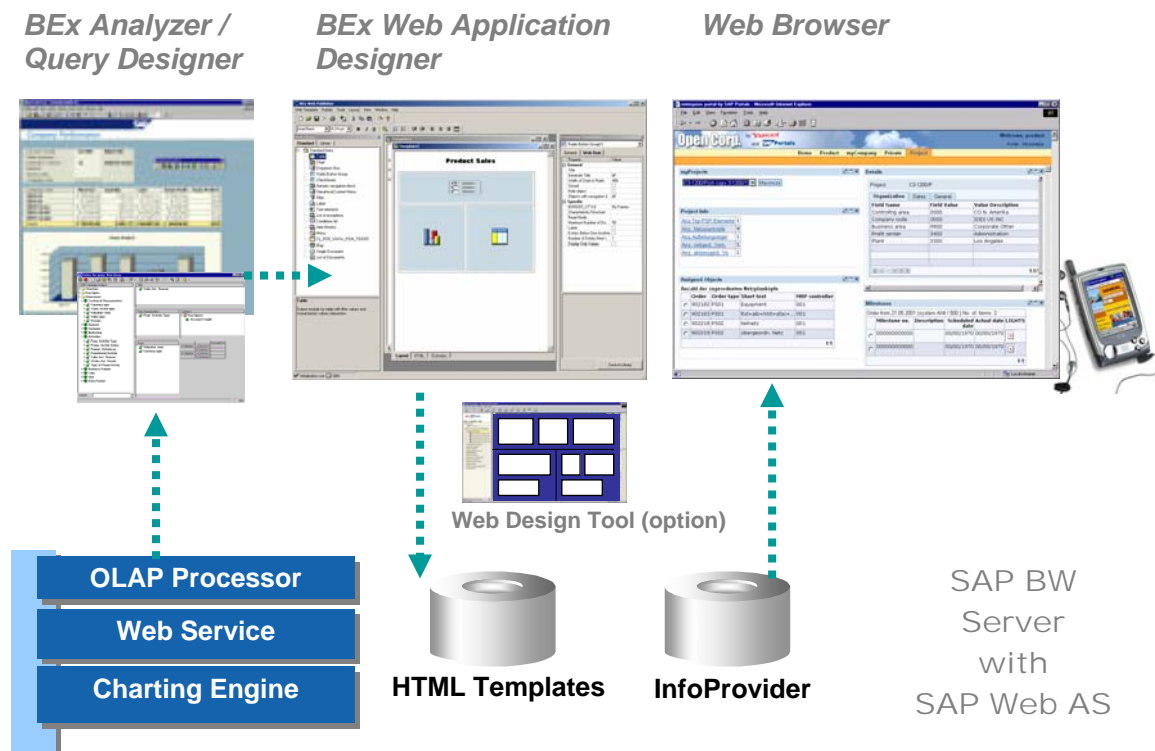
ADK-based archiving occurs independently of the underlying tables. By moving data out of SAP BW into independent memory systems, shorter load and query cycles and significant cost savings of up to 90% can be obtained because of the reduced demand on disk storage. For analysis purposes the archived data has to be loaded back into SAP BW.

2.6 Views / Reports

2.6.1 Reporting Tools

The basic principle of SAP BW is to provide information on processes relevant to decision making for almost all functions within an enterprise. For this purpose, SAP BW includes reporting tools, the Business Explorer tools, in order to report on and present centrally stored data that may come from different sources.

Business Explorer Web Application Framework



With the Business Explorer tools you are able to

- Create reports,
- Execute predefined reports,
- Define calculated and restricted key figures (for example key performance indicators)
- Analyze and present data.

The following Business Explorer components / tools are available for different user types and purposes:

BEx - Query Designer

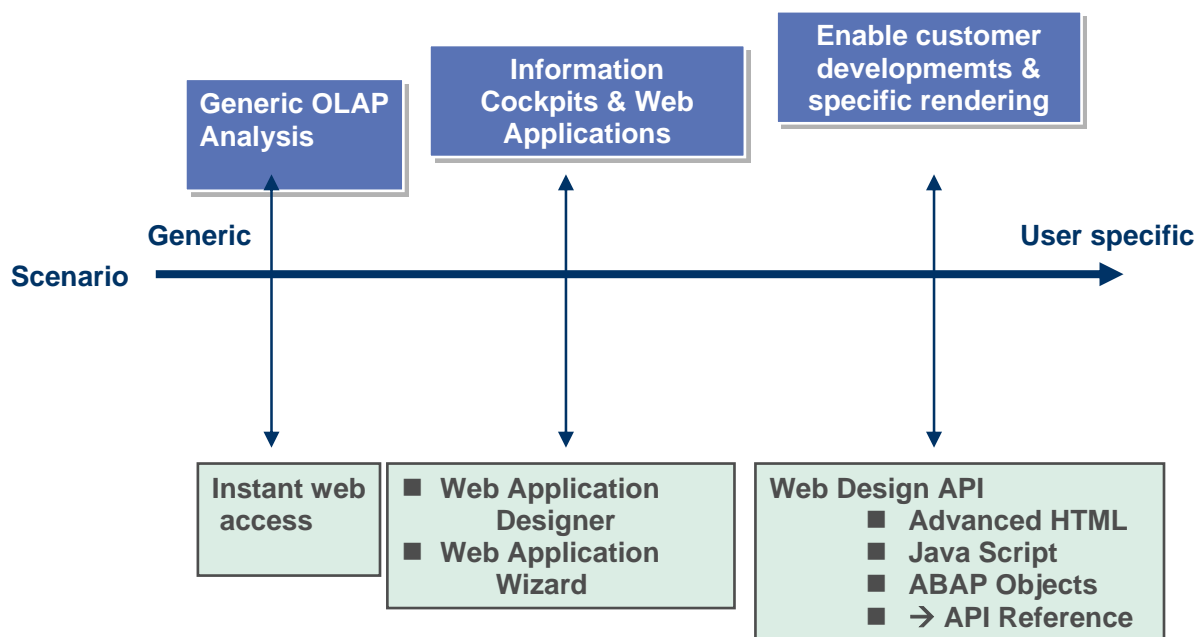
With the Query Designer reports or queries can be generated for all data stored in BW. The Query Designer can be called via the Web or MS Excel or it can be defined as a desktop application.

BEx Web Application Designer

The BEx Web Application Designer (SAP BW 3.0B) and the Web Application Wizard that is integrated into it allow you to define individual Web Applications. By using queries and HTML-documents, information can be generated and presented for publishing in the Intranet or Internet.

The following overview shows the broad spectrum of the BEx Web Application Designs:

BEx Web Continuum



BEx Analyzer

The reports generated with BEx Query Designer can be transferred to Excel via the BEx Analyzer and can be uadapted e.g. for presentations.

BEx Browser

This is a reporting menu (similar to a portal), from which the end user can call the analyses produced by the other Business Explorer tools.

Formatted Reporting

Formatted reporting involves the integration of Crystal Decisions into BW. With this form of reporting, reports can be generated with pixel-exact layouts, for example, for predefined forms.

Accessing Reports

Reports created with various different BEx tools can be easily integrated into a portal using iViews.

2.6.2 Reporting Options

The key figures and characteristics from one or more InfoProviders that are required in a report are collected using Drag & Drop.

The basic functions *drilldown* and *drillup* are used for navigating in multidimensional data structures such as InfoCubes. *Drilldown* is the ability to analyze compressed data corresponding to its hierarchy level in the underlying sub-result. The end user is able to navigate down through the various levels in the hierarchy of compressed data (*drilldown*) and vice versa (*drillup*).

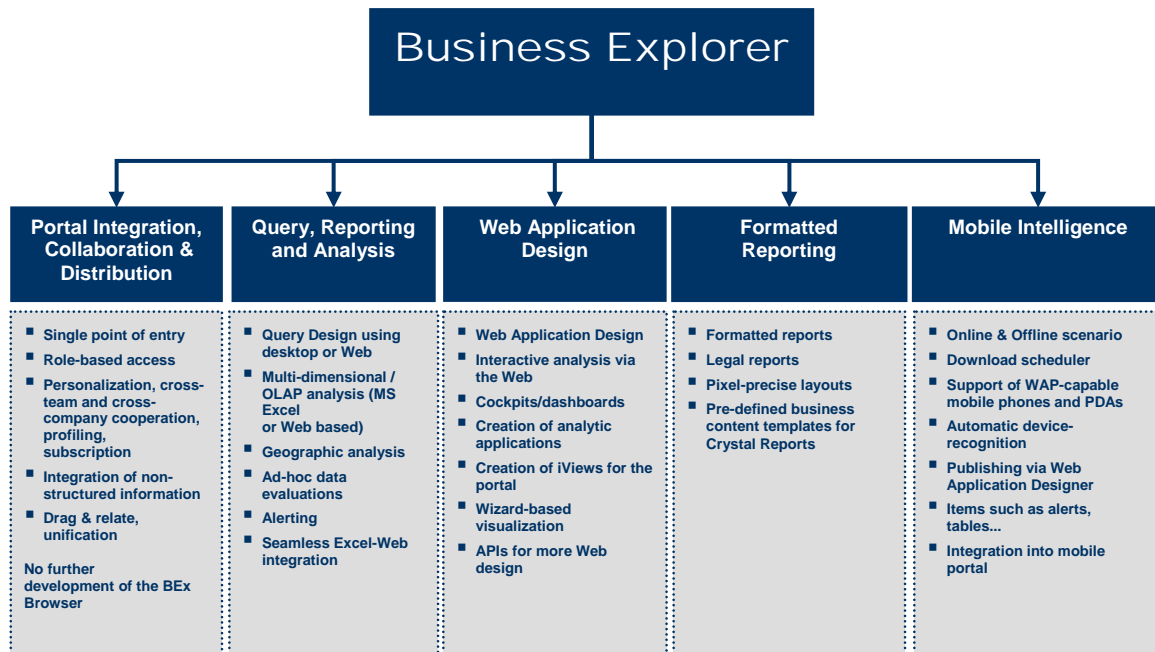
In addition to the navigation functionality previously allowed, it is now also possible to navigate from one report to another. This report may be based on the same InfoCube or on a different InfoCube (*drill-across*).

The *drill-through* functionality allows you to access the operative dataset from reporting. You can jump from a report to the stored document level of the operative dataset, or you can access the underlying transaction of an SAP component from there.

Personal Data

When loading data into a data warehouse you have to check whether detailed personal data needs to be extracted. If this is deemed necessary by the enterprise, you have to ensure, for example using access authorization controls, that only authorized end users can access personal data. *Drilldown* or *Drill through* functionality to data on individuals should only be allowed for authorized end users.

2.6.3 Access Rights with Self-Developed Reports



The authorization check at data level takes place in SAP BW.

When integrating reports/ views of the InfoSources and InfoCubes into the *Portal*, data/reports are included in the respective portal and where necessary, linked to other data in the portal using the appropriate connections.

In this case, access to data is also protected by the roles in the portal in question. **In this case the data protection official is also responsible for the roles that have to be defined in the portal and the defined *Drag and Relate* correlations.**

In the case of *queries and views* mentioned above, read access to the InfoCubes and InfoObjects by queries is protected by special authorization objects. Change access to queries is controlled with authorization objects S_RS_COMP and S_RS_COMP1. The authorization to create and change the assignment of queries to user groups is also controlled with this authorization object. Creating and changing views to InfoCubes is dealt with using objects S_RS_ICUBE and S_RS_IOBJ.

These objects allow you to distribute the authorization to

- create/change/restrict views of the data,
- generate/ change queries and assign queries to users, and
- call fixed predefined queries

to various roles to be viewed by 2 or 3 people.

The data protection official is responsible for the abstract distribution of roles and the actual definition of the corresponding roles.

Web applications are created using the BEx Web Application Designer. You can create HTML pages that contain BW-specific content, as well as tables, charts or maps. Web applications can be saved as URLs and then accessed via the Internet, Intranet or with mobile devices. If Web applications are saved as iViews they can be integrated into company portals.

Access to Web applications that are created in this way is protected using the standard BW authorization objects (see chapter 2.7.2.3). The tool, the Web Application Designer itself, can be protected using authorization object S_RS_TOOLS. A small modification is necessary (see SAP Note 605417).

If you are using mobile devices with the *BEx Mobile Intelligence* tool you are also able to call reports that have been generated whilst traveling using the BEx Web Application Designer. An authorization check takes place using the standard BW authorization objects (see chapter 2.7.2.3).

Finally, as well as the Business Explorer reports that are available online with *Web Applications* and *Mobile Applications*, it is also possible to call reports offline. The BEx Download Scheduler enables you to download precalculated HTML pages to a desktop PC, or a PDA device. An authorization check then takes place using the standard BW authorization objects (see chapter 2.7.2.3). Data saved to the front end has to be protected locally (for example, encoding, password protection).

2.6.4 Business Content Reports

In addition to the scope of Business Content as described in chapter 2.1.6, this section is to exemplify the reporting possibilities and roles (that have assignments made to them in BC) and consider them from the point of view of the legal requirements of a data warehouse.

The advantage of this program and “complete“ data solution is that it uses already existing information models.

However, from the perspective of the data protection requirements made on a BW, we cannot talk about a “complete“ solution at all..

In the BC information modules there is a large amount of personal data and/or data that can refer to individuals (for example sales group and sales representative in profitability analysis (CO – PA), work center with actual – and – debit - amounts, with exact turnaround/execution times, actual and debit performance efficiency rates, with individual work processes, etc.).

From the point of view of data protection, there is the risk that BW users may take on the “complete solution“ of BC, without executing any further checks as to the admissibility of the data from the perspective of data protection requirements.

To clarify this, particular examples will now be given. The aim here is not to offer a full list of queries that process personal data. The aim is to highlight that when implementing Business Content

- the admissibility of data in the operative system has to be checked by the person responsible
- processing still needs to take place within the context of the original purpose

- one must check whether new determinations of purpose can be pursued by combining data from Business Content
- the authorization concept for personal data between the operative system and the BW Business Content has been illustrated 1:1, as necessary

The BC contains information models for the following applications – and queries (reports) – in the sense mentioned above (current as of BW Release 3.0 A):

- Analytical applications
- Customer Relationship Management
- Supplier Relationship Management
- Supply Chain Management
- Product Life – Cycle Management
- Financials
- Human Resources
- Exchanges
- Industry Solutions (for 17 industries)
- Country – Specific Content
- Demo Content
- Cross-application components

For these areas the information models named above are determined, normally with the following structure:

- Roles
- Queries
- InfoSources
- DataSources
- InfoCubes
- ODS – Objects
- Key figures
- Characteristics
- Workbooks

A complete list of the personal data would be too extensive for this guide.

In the following we are restricted to providing an example of how "non-HR" and "HR" queries are handled as BC

In SAP BW there are similar techniques to finding personal data to those in R/3. In R/3, the tables with personal reference are analyzed with the ABAP dictionary via domains, in SAP BW, the information is attained from the InfoObjects with the Administrator Workbench, for example, *Ovendor*, *Ocustomer*, *Oemployee*. Similar to the ABAP Dictionary, there are where-used lists here as well.

Because the Administrator Monitor Workbench is a privileged tool for Administration, we recommend that these functions also be performed by them.

2.6.4.1 Examples from Non-HR Applications

DemoCube Profitability Analysis (CO – PA) (technical name: 0D_CO_PA)

The DemoCube for the profitability analysis (CO-PA) serves as the data basis for delivered DemoQueries for reports in profitability and sales accounting, for example.

The query contains personal data, such as „Sales Group“ (0D_SALE_GRP), which, in connection with sales quantity (0D_QTY), enables performance measurement/evaluation that may touch on rights of co-determination.

PSP Element : Costs/Variiances (technical name: OPS_C01_Q0002)

This query offers an overview of the costs accrued on a PSP element. It enables analysis of these costs in actual and planned according to cost type and provides the absolute variance from planned costs in the respective currency and in percent.

Depending on the degree of detail of the PSP element (a PSP element is assigned to a person), a personal reference can result that can enable a performance check.

Overview Report – Projects (technical name : OPS_C01_Q0004)

With the help of this query, you receive an overview of the development status of the projects you select. The query compares actual and planned costs, actual and planned work and order start and order end dates for the selected projects.

Personal data is also present among the general conditions described for a PSP element and a performance measurement/evaluation is possible that may touch on rights of co-determination.

Performance Efficiency Rate (technical name : OPP_C03_Q011)

This query compares the target performance efficiency rates and the actual performance efficiency rates on the job. It thus displays how effectively a job is being done.

If a person or a (small) group of people can be assigned to a job, this becomes personal data because a performance measurement/evaluation can be done, thus touching on rights of co-determination.

Actual Quantities for a Job (technical name : OPP_C04_Q002)

This query displays the delivered lot size, the confirmed quantity and the confirmed scrap for a specific period.

Refer to the lists of examples above.

These few examples – also directly from personal data – from the Business Content areas,

- Product life cycle management
- Program & project management

and

- Supply chain management
- Production

demonstrate the need to check and evaluate the BC in a legal regard before it is used and to introduce and implement the necessary measures, such as de-personalization, aliasing, checking and, as required, adjusting the authorization concept.

2.6.4.2 Business Content for HR Data

The multi-dimensional views in SAP BW enable one to cover many classic standard reports with a single mySAP HR query.

Because of this, the mySAP HR Business Content includes, for example, an illustration of the headcount based on organizational characteristics, such as the organizational structure of the company, employee groups, personnel areas and cost centers. In addition, personal characteristics such as gender, age or nationality are also displayed.

Due to the free combination of all characteristics with this query, detailed information display down to the individual employee is possible.

There must be a legal foundation for saving and using this data for all of the purposes that are possible with these tools. SAP AG has not checked this yet. If this legal foundation is not present, the data must be aggregated, de-personalized or aliased.

A further task of the data protection official for Business Content in HR is to ensure that, in personnel planning throughout the company, only aggregated data on headcount, personnel movement, or employee structure be transmitted. Personal details such as age, gender, nationality, skills or education should not be present in the source systems.

Another main point is the user authorization concept (see chapter 2.8.2.4.).

The „standard roles” available in Business Content are – in contrast to the standard roles that are kept quite general in the „general“ BW – specifically tailored to tasks and contain the queries necessary for these roles.

Here is an example of the data protection relevance of „standard” reports and roles in Business Content HR for the Time and Labor Data Controller:

Time and Labor Data Controller (Technical name: SAP_BW_0ROLE_0024)

The *Time and Labor Data Controller* provides data that enables monitoring of time and labor data in view of strategic company objectives. It creates reports, for example on the work done by all departments/employee groups or the development of overtime.

Reports on this type of data enable, for example, control of overtime and the productivity of individual enterprise areas.

This role includes the following activities in personnel time management:

- Statistics on absences, productivity and overtime
- Analyzing remaining vacation days and other entitlement to paid absences

The following workbooks are available for the *Time and Labor Data Controller*. Every task corresponds to a cluster of several workbooks. The workbooks contain one or more queries that deliver the relevant information.

Task (Cluster)	Workbook
Key Figures for Time and Labor Data	Cost center debit in annual comparison
	Time and labor data monthly development
	Time and labor data overview compared to previous year
	Time and labor data expressed in full-time employees
Overview of Time and Labor Data	Productivity rate
	Overtime rate
	Illness rate
	Leave per planned
	Leave taken in units of full-time equivalence

These workgroups enable – if not restricted during adjustment of roles – drilldown to individual employees.

The first thing that needs to be clarified is the question that is often addressed regarding the eligibility of personal data. If it appears that the eligibility conditions are not fulfilled, this data may not be processed and used in BC HR.

If there is, in fact, legal permission given, you need to check whether the roles provided in BW actually reflect the actual organizational and task-specific situation of the user's company, or whether the authorizations that are supplied with this role are too extensive. „Restrictions“ of authorizations, for example for specific personnel areas or employee groups, and so on, are required.

The following roles are currently available in Business Content HR (basis is documentation for SAP BW Release 3.0A 2001):

- **Recruiter** (Technical name: OROLE_0020)

The role of the *Recruiter* includes all administrative activities and data entry tasks in the area of the *Recruiter* component.

- **Human Resources Analyst** (Technical name: OROLE_0021)

The *Human Resources Analyst* is viewed as a strategic business partner of human resources and corporate management. He has expert knowledge and knows how to align HR policies with the company's strategic objectives.

- **Payroll Manager** (Technical name: OROLE_0023)

The *Payroll Manager* is responsible for the complete payroll area (processing, monitoring, follow-up activities, etc.).

Key figures and reports from payroll support him with analysis and with subsequent decision making.

- **Benefits Expert** (Technical name: OROLE_0027)

The *Benefits Expert* is viewed as a strategic business partner of the HR Manager and line manager. The planner has expert knowledge and knows how to align the personnel policy with the company's strategic objectives. The planner solves problems using HR-based methods of resolution and significantly involved in operational implementation of these solutions.

- **Organizational Planner** (Technical name: OROLE_0025)

The *Organizational Planner* (OP) is seen as a strategic business partner of the HR Manager and the line manager. The planner has expert knowledge and knows how to align the personnel policy with the company's strategic objectives. The planner solves problems using HR-based methods of resolution and significantly involved in operational implementation of these solutions.

The OP is also responsible for system process analysis and design. The focus of these activities include quality improvements, data management, process improvements and/or re-engineering.

- **Training Expert** (Technical name: OROLE_0022)

Training Expert is seen as a strategic business partner of the HR Manager and the line manager. He has expert knowledge in the training area and knows how to align education and further training with the company's strategic objectives. The expert is responsible for all planning tasks and the overall coordination of education activities in the company. In this regard, the evaluation of relevant education data is important.

- **Personnel Development Manager** (Technical name: OROLE_0028)

The *Personnel Development Manager* is an expert in *personnel development* and is viewed as a strategic business partner of the HR manager and the line manager. He has expert knowledge and knows how to align personnel development with the company's strategic objectives. His general task is to transfer strategic corporate specifications

into personnel development concepts and methods of resolution and to implement them. In this regard, the evaluation of relevant data for personnel development is important (that is, on qualifications and evaluations).

- **Compensation Management Expert** (Technical name: OROLE_0026)

The *Compensation Management Expert* develops and leads the introduction of compensation programs that offer employees competitive salaries, motivation and rewards.

These focus on programs for monetary remuneration (salary, bonus) and programs for quasi-monetary remuneration (long-term compensation plan) for workers and employees

- **Personnel Cost Planner** (Technical name: OROLE_0030)

The *Personnel Cost Planner* is responsible for the analysis of various cost scenarios. The key figures and reports from personnel cost planning support him in his analysis and in making subsequent decisions.

- **Employee Relations Manager** (Technical name: SAP_BW_OROLE_0029)

The *Employee Relations Manager* leads negotiations with employers, employees and unions. The manager's task is to negotiate and fix wage levels, to present logs and reports and to advise and train managers in the works council and union work areas.

The role of the *Employee Relations Manager* is specific to Asia and the US. In other countries, such as Germany, the tasks or some of the tasks of the *Employee Relations Manager* can be performed by the personnel officer, the union agent or the works council agent.

- **Travel Manager** (Technical Name: OROLE_0032)

Reporting from the BW Business Content supports the travel manager in evaluating data on planned and past trips and invoicing. By using BW, the manager can immediately and easily find information on travel destinations, transactions with hotel chains and rental car companies or statistics for expense documents, for example.

- **HR BW Web Cockpits** (Technical Name: SAP_BW_OROLE_0019)

From a technical viewpoint, this role is available to assign the Web Cockpits for *Human Resources Management* (HR) to a user. The HR Web Cockpits provide, among other things, Business Content for the Business Package *Manager Self-Service*.

One needs to ensure that these roles correspond to the user's existing tasks. You should avoid using general roles with very extensive authorizations. Data protection officials have to make sure that these roles and their authorizations are adapted to the operational realities and situations, in order to fulfill the admissibility prerequisites or to guarantee the imperative of limited use. and its technical assurance.

The ETL process (extract, transform and load) described in chapter 2.5 provides the official with an important opportunity to check the admissibility of processing and use of data.

2.7 Implementation of the Requirements from Section 9 BDSG and Appendix: Technical-Organizational Measures

2.7.1 Requirements

In this section, the technical-organizational requirements for recording, processing and use of personal data and checks of such data will be discussed. The requirements are to be fulfilled in general, that is, outside of the area of application of national laws. These provisions do not only refer to productive systems, but also to pre-loaded systems that contain accessible personal data or where settings are prepared that are later to be transported to the production environment.

Based on EU directive 95/46/EG, the required technical-organizational measures have been expanded to provide protection against - on the one hand - accidental or unauthorized destruction and accidental loss of data (7: Availability Control) and - on the other hand - to guarantee specific circumstances of processing (part 8).

Reference: The valid legal requirements from Section 9 BDSG, along with an overview of SAP functionality to fulfill these requirements can be found in Chapter 4.1. of the *Data Protection Guide for SAP R/3*. An overview of the connection between the two guides is provided in 2.7.2.11.

2.7.2 SAP-Facts, Risks and Measures

2.7.2.1 Identification and Authentication

Before users can access the information and functions in the R/3 system, they have to log on with a user ID and password. In contrast to the administrator, the end user does not generally log on directly in the Business Warehouse. Instead they obtain the required entry through the portal or through the front end. When the authentication data is entered, the user is identified by R/3 and the system checks whether the user is authorized to work with the system.

Reference: The rules valid here, along with notes for the corresponding secure settings for password creation are described in chapter 4.2.1. of the *Data Protection Guide for SAP R/3*. When a portal is used, further measures are to be made and monitored regarding authentication.

2.7.2.2 Standard User

Within BW, as in R/3, there are a total of four standard users (SAP*, DDIC, SAPCPIC, EARLYWATCH) that should be provided with special protection regarding the organizational-technical measures that are to be taken.

Reference: Chapter 4.2.2. of the *Data Protection Guide for SAP R/3*.

2.7.2.3 User Authorization Concept: Authorization Objects for BW

Basic Access Control

Access protection for a BW system is built on the basis of authorization objects. SAP provides a standard 300 of them. Of those, the authorization objects for the following object classes of special significance for ensuring an effective authorization concept for protecting personal data:

Object Class	Description
AAAB	Cross-application authorization objects
BC_A	Basis – Administration
BC_C	Basis – Development environment
BC_Z	Basis – Main functions
HR	Human resources
RS	Business Information Warehouse
RSR	Business Information Warehouse - Reporting (user-defined authorization objects)

The following presents all authorization objects from the object class RS „Business Information Warehouse“. The complete documentation for the authorization objects is available on menu path

Tools -> Administration -> User Maintenance-> Information System -> Authorization Objects (all objects for object class RS)

or via the profile generator (PFCG).

BW Authorization Objects

Generally, the specific BW authorization objects can be divided into the following types:

- Restrictions within the Administrator Workbench
- Restrictions within the Business Explorer
- Restriction of reports to certain content specifications (transaction RSSM)

A special feature of BW systems should be mentioned: in addition to the standard authorization objects, users can create their own authorization objects that depend on personal data. The transaction RSSM is available in the system for this purpose.

The authorization objects that the user has created provide the necessary basis to create technical measures for access protection that are specifically for the defined information and data structures - for example regarding InfoCubes, in order to create a restriction of access rights on the field level, for example. The objects particularly refer to reporting functions and ensure that the organization can establish which of the personal data in BW is available to the user.

Authorization Objects for Administrator Workbench	Fields / Restrictions
<p>S_RS_ADMWB</p> <p>Administrator Workbench - Objects</p> <p><u>Purpose:</u> Restriction to specific objects within the Administrator Workbench</p>	<p><u>Determination of Access Type</u></p> <p>Display, maintain, execute, update</p> <p><u>Determination of the objects to be processed</u></p> <ul style="list-style-type: none"> → Source system → InfoObject → Monitor → Application components → InfoArea → Administrator Workbench → Settings → Metadata → InfoPackage → Reporting-Agent setting → Documents
<p>S_RS_HIER</p> <p>Administrator Workbench - Hierarchy</p> <p><u>Purpose:</u> Restriction to hierarchy levels within administration</p>	<p><u>Determination of access type</u></p> <p>Display, maintain, report</p> <p><u>Determination of InfoObject</u></p> <p><u>Determination of hierarchy names</u></p> <p><u>Determination of hierarchy version</u></p>

Authorization Objects for Administrator Workbench	Fields / Restrictions
<p>S_RS_ICUBE</p> <p>Administrator Workbench InfoCube</p> <p>Purpose: Restriction to InfoCubes</p>	<p><u>Determination of access type</u></p> <p>- Display, delete, maintain, update</p> <p><u>Determination of InfoArea</u></p> <p><u>Determination of InfoCube</u></p> <p><u>Determination of Subobjects for InfoCube</u></p> <p>→ Definition → Update rules → Aggregate → Export → Export Data source</p>
<p>S_RS_IOBC</p> <p>Administrator Workbench InfoObject Catalogs</p> <p>Purpose: Restriction to InfoObject catalog</p>	<p><u>Determination of access type</u></p> <p>- Display, maintain</p> <p><u>Determination of InfoArea</u></p> <p><u>Determination of InfoCatalog</u></p>
<p>S_RS_IOBJ</p> <p>Administrator Workbench InfoObject</p> <p>Purpose: Restriction to InfoObject</p>	<p><u>Determination of access type</u></p> <p>- Display, maintain</p> <p><u>Determination of InfoObjectCatalog</u></p> <p><u>Determination of InfoObject</u></p> <p><u>Determination of Subobjects for InfoObject</u></p> <p>→ Definition → Update rules</p>

Authorization Objects for Administrator Workbench	Fields / Restrictions
<p>S_RS_IOMAD</p> <p>Administrator Workbench - Master Data</p> <p><u>Purpose:</u> Restriction of master data maintenance within the Administrator Workbench</p>	<p><u>Determination of access type</u></p> <p>- Display, maintain</p> <p><u>Determination of InfoObjectCatalog</u></p> <p><u>Determination of InfoObject</u></p> <p><u>Determination of sub object for InfoObject</u></p> <p>→ Definition → Update rules</p>
<p>S_RS_ISET</p> <p>Administrator Workbench - Infoset</p> <p><u>Purpose:</u> Restriction to Infosets</p>	<p><u>Description of access type</u></p> <p>- Display, maintain</p> <p><u>Determination of InfoArea</u></p> <p><u>Determination of Infoset</u></p> <p><u>Determination of sub object for Infoset</u></p> <p>→ Definition → Data</p>
<p>S_RS_ISOUR-</p> <p>Administrator Workbench - InfoSource Flexible Update</p> <p><u>Purpose:</u> Restriction to InfoSource with flexible update</p>	<p><u>Determination of access type</u></p> <p>- Display, maintain, request</p> <p><u>Determination of application components</u></p> <p><u>Determination of InfoSource</u></p> <p><u>Determination of subobjects for the Infoset</u></p> <p>→ Definition → Communication structure → Transfer rules → Data → Info Package → Metadata</p>

Authorization Objects for Administrator Workbench	Fields / Restrictions
<p>S_RS_ISRCM</p> <p>Administrator Workbench - InfoSource direct update</p> <p><u>Purpose:</u> Restriction to InfoSource with direct update</p>	<p><u>Determination of access type</u></p> <p>- Display, maintain, request</p> <p><u>Determination of the application component</u></p> <p><u>Determination of InfoSource</u></p> <p><u>Determination of sub object for Infoset</u></p> <p>→ Transfer rules → Data → Info Package → Metadata</p>
<p>S_RS_MPRO</p> <p>Administrator Workbench - MultiProvider</p> <p><u>Purpose:</u> Restriction to Multi Provider</p>	<p><u>Determination of access type</u></p> <p>- Display, maintain</p> <p><u>Determination of InfoArea</u></p> <p><u>Determination of MultiProvider</u></p> <p><u>Determination of sub object for MultiProvider</u></p> <p>→ Definition → Export DataSource</p>
<p>S_RS OSDO</p> <p>Administrator Workbench - ODS Object</p> <p><u>Purpose:</u> Restriction to ODS</p>	<p><u>Determination of access type</u></p> <p>Display, maintain</p> <p><u>Determination of the InfoArea</u></p> <p><u>Determination of ODS Object</u></p> <p><u>Determination of subobjects for ODS</u></p> <p>→ Definition → Update rule → Data → Export DataSource</p>

Authorization Objects for Business Explorer	Fields / Restrictions
<p>S_RS_COMP</p> <p>Business Explorer - Components</p> <p><u>Purpose:</u></p> <p>Restriction to specific components for the Business Explorer for the query definition</p>	<p><u>Determination of Access Type</u></p> <p>Insert, change, display, delete, execute, enter</p> <p><u>Determination of InfoArea</u></p> <p><u>Determination of InfoProvider</u></p> <p><u>Determination of reporting component</u></p> <p><u>Determination of component type</u></p> <p>→ Query (REP)</p> <p>→ Structures (STR)</p> <p>→ Calculated key figures (CKF)</p> <p>→ Restricted key figures (RKF)</p>
<p>S_RS_COMP1</p> <p>Business Explorer - Components: Expansion to Owner</p> <p><u>Purpose:</u></p> <p>With this object, you have the option of making queries from specific owners (creator of the query) accessible only to specific users for display or editing (in connection with S_RS_COMP)</p>	<p><u>Determination of access type</u></p> <p>Change, display, delete, execute, enter</p> <p><u>Determination of reporting components</u></p> <p><u>Determination of component type</u></p> <p>→ Query (REP)</p> <p>→ Structures (STR)</p> <p>→ Calculated key figures (CKF)</p> <p>→ Restricted key figures (RKF)</p> <p><u>Determination of owner</u></p>
<p>S_RS_FOLD</p> <p>Business Explorer - Folder on or off</p> <p><u>Purpose:</u></p> <p>Turning the general view on or off on the InfoArea folder.</p>	<p><u>Determination of folder view</u></p> <p>SUP_FOLDER = „X“, to hide the <i>Folder</i> button, otherwise leave the field empty or set to „*“...</p>

Authorization Objects for Business Explorer	Fields / Restrictions
S_RS_TOOLS Business Explorer - individual tools <u>Purpose:</u> Restriction to certain user communities	Determination of „logical command name“ Currently the authorization object has no effect, the check can be activated for the BEx Web Application Designer as a modification (see Note 332738 and 605417).

Authorization objects for Report Authorizations	Fields / Restrictions
S_RSR_...	BW Reporting Authorization Technology to define authorizations independent of content in BW - Use authorization variables - Indicate InfoObjects as authorization relevant - Activate InfoCubes - Include authorization variables in queries - Use of transaction RSSM - Peculiarities of hierarchy authorizations

System Authorizations

In addition to the BW authorization objects listed above, system-related authorization objects are tested with transactions in the BW system. These are contained in the same object classes as in the standard R/3 systems. This means that there are comparable risks associated with these authorizations and the measures to be taken are also similar.

The BW-specific debugging tool RSRTRACE is protected by the transaction code. During execution, all of the programmed authorization checks are carried out. The same precautions are valid as those for debugging in a standard R/3 system.

Reference: *Data Protection Guide for SAP R/3*, Chapter 4.2.3.

However, not all authorization objects are available in BW systems that are delivered in R/3 systems. For example, the object P_ORGIN (HR master data) is not available in BW systems.

Customer-defined authorization objects are required for differentiated reporting (S_RSR_* or Z*-objects). In this regard, access protection differs greatly between BW and R/3 systems. In the latter, there is a number of authorization objects available for reporting functions in the standard delivery. BW systems are more flexible due to their architecture, which means that special technical measures are required for reporting with customer-defined authorization objects. The creation of the BW authorization concept thus requires a considerable effort, and this should be planned for in the project.

The access rights, which should be kept restrictive, may not be undermined by system authorizations. You should be aware of this even in the data modeling stage. Important, low-level authorization objects related to this include, for example:

- S_TABU_DIS Table maintenance or display (using standard tools such as for example, SM30, SE16)

Note: PSA and ODS contain the data in plain text so that it can be read with SE16. This is not possible with data from the InfoCube because it is in INTEGER format.

- S_DEVELOP Programming, all queries / ABAPs can be changed with SE38.
- S_TCODE Transaction code check upon transaction start
- S_QUERY SAP query authorization.

Functions that are quite significant from a data protection point of view, such as loading data from the source system or from multiple source systems, and maintenance or display of InfoAreas and InfoObjects can be authorized using BW authorization objects. The following authorization objects should be listed here:

- S_RS_ADMWB Administrator Workbench - objects
- S_RS_HIER Administrator Workbench - hierarchy
- S_RS_ICUBE Administrator Workbench - InfoCube
- S_RS_IOMAD Administrator Workbench - maintain master data

2.7.2.4 User Authorization Concept: Roles for the BW

In BW - as with after Release 3.1G of the R/3-Classic - the **Profile Generator** (transaction PFCG) is available as a tool for automating the creation of rights. The underlying term here is the **Role**, called **Activity Group** in older releases; it is possible to combine individual and **composite roles**.

Like with the authorization profile, the activities for the individual tasks for the functions to be accomplished are combined using roles. The required rights are automatically (menu supported) created using the profile generator.

Implementation of the determined requirements takes place in sub steps:

- Determination of the required work centers in terms of establishing tasks divided by function for the respective user groups with division
- Determination of the required transactions and / or use of the standard roles provided by SAP by work center
- Rework of the automatically proposed authorizations
- Generation of profiles and authorizations

- Creation/maintenance of user master records
- Test through user departments, as needed, making adjustments
- Afterwards, release by user department
- Transport of roles into the productive system

In order to protect personal data, a properly designed authorization concept is necessary for the entire BW system landscape and thus for the development, quality assurance and productive systems. The respective roles should only be used productively once the test and acceptance procedure has confirmed the effectiveness of the access protection measures.

In addition to the standard roles provided by SAP, they are also continuing to provide standard profiles (for example, SAP_ALL or SAP_NEW). For security reasons, these should not be used.

Reference: *Data Protection Guide for SAP R/3*, Chapter 4.2.4

In order to carry out system support tasks, similar roles (including user administration, system monitoring, and operating) should be created, as in R/3 classic. The system support agent, who checks the correctness and completeness of the data transfer and who must initiate any necessary corrections in a timely manner, has a special significance in the BW environment.

SAP provides around 500 standard roles, on the one hand for use in BW, and on the other for BW administration. Currently these are being kept quite general and have to be enhanced to suit the needs of the company using them.

Depending on the amount of information used and on the reporting requirements, companies can develop their own roles for reporting.

2.7.2.5 User Authorization Concept: Effective Design

In comparison to R/3 classic systems, there are special risks from a data protection viewpoint in BW installations. They can be found

- in the system interfaces, since a BW system draws its data from pre-loaded systems in a certain periodicity (input control),
- in the transformation requirements and change options for personal data in the BW system (input control) ,
- in the special methods for data retention and reporting options (access control) and
- in the combination of data from multiple source systems when new reporting options result in the BW system. Measures in the authorization concept are of priority here to be able to separately process the data retrieved for different processes.

In the following, an example demonstrates which work centers can be differentiated using the authorization concept. It is important to note here that the rights to be assigned per work center regularly differ depending on whether they are set up for development- / quality assurance or productive system. Furthermore, roles should be created for the SAP source systems that are responsible for data export. If SAP external source systems are being used access protection measures should also be considered for the source systems.

For the „user“ work center, a clear dissection should be made regularly on personal data according to measures for the current tasks and capacities for differentiated reporting.

Work Center	Rights to Be Assigned (Examples)	Rights Not to Be Assigned (Examples)
User	Execute existing reports, where the work centers are to be distinguished according to measures for the specific reporting requirements	Definition of reports Creation / maintenance of users / roles
Developer department	Definition of reports; Creation / maintenance of queries as needed; Customizing as needed (only in the development system)	System administration (esp. transport of changed objects); Creation / maintenance of users / roles
Developer IT	Customizing (only in development system); Administration of workbench	System administration (esp. transport of changed objects); Execution of existing reports
Quality assurance	Display of InfoCubes; Checking the PSA (Persistent Staging Area)	Definition of reports Customizing
Basis- / System-Administration	Administration of the Workbench; Loading data from the source system; Transport of system changes / roles	Customizing Definition of reports Creation / maintenance of users / roles
Database Administration	Maintenance of database parameters	Definition of reports Creation / maintenance of users / roles
User Administration	Creation / maintenance of users	Definition of users Creation / maintenance of roles
Authorization Administration	Maintenance of roles (PFCG + RSSM)	Definition of reports Creation / maintenance of users
Revision/Data Protection	Display of users; Retracing major settings / security parameters; Retrace transformation rules	Definition of reports Creation / maintenance of users / roles
ALE Remote (Background User)	Loading data from the sources system as a background user	Creation / maintenance of users / roles
Emergency (Assignment included in an emergency concept)	All access rights	None

2.7.2.6 Special Features of Authorization Check

In BW, in relation to deactivating authorization checks (transaction SU24, authorization objects under transactions SU25 / SU26 upgrade tool for the profile generator), the protection of program codes (authority check) and the protection of reports using authorization groups / assignment to transactions, these all follow the same rules as in R/3 classic.

Note that especially the RSR objects (objects created by the user with RSSM) can also be deactivated.

Reference: The facts and risks that are valid here can be found in chapter 4.2.5. of the *Data Protection Guide for SAP R/3*.

In addition, in regard to authentication, further measures are to be made and monitored when using a portal.

Once again, it must be pointed out that there are further protection options when a user creates his own authorization object and a detailed reproduction must also be implemented.

2.7.2.7 User and Authorization Administration

Generally there is no difference in user administration between the R/3 classic and the BW, which means that processes that have already been realized - by using the profile generator - can also be valid for BW.

Reference: Chapter 4.2.6 of the *Data Protection Guide for SAP R/3*

Supplemental to the guide, the following four authorization objects are available. They control the use of certificates, options for deactivating authorization objects and the use of a central user administration:

- Certificate registration, certificate request and assignment (S_USERCERT)
- Authorization system: Globally deactivate authorization objects (S_USER_OBJ)
- Users: System-specific assignment authorization objects (S_USER_SAS)
- User master record: System for central user maintenance (S_USER_SYS)

Additionally a role should be created in rights administration for using transaction RSSM to create new authorization objects.

2.7.2.8 Changes to the Productive System

To ensure the logging of changes, you should make the same settings as in R/3 classic: Change and Transport System, table logging / Customizing, system changeability (transaction SE06), logs (on the corresponding databases), table T000.

Reference: Chapter 4.2.7 of the *Data Protection Guide for SAP R/3*

Data changes in the BW productive system have a special significance because the BW should primarily be viewed as a reporting tool (see 2.8.2.9). It is important to give special mention to the function module RSAR_ODS_API_PUT.

Options for changing transferred original data: The transferred data is first loaded into a persistent storage area (PSA) and then it is updated to the data targets (InfoCubes). The PSA data is visible to the administrator for debugging purposes. When there is an erroneous update, there is no option of changing the data.

However, if the data update from the PSA to a data target was not successful, that is, there was an erroneous request, for example due to inadmissible values in the form of special characters, the PSA data can be changed and then updated manually. Because this process is not logged, these changes should be documented accordingly. As an alternative, in case of error, the request can be deleted from BW completely and reloaded after eliminating the cause of the error.

For data protection reasons, this option is preferable to ensure an identity between received and transferred data.

The principle use of this change option is protected by BW authorization objects (S_RS_ISOUR).

2.7.2.9 System Interfaces

For communication between a BW and an external system (SAP or non-SAP systems), similar options are available as are present in R/3 classic.

Reference: Chapter 4.2.8 of the *Data Protection Guide for SAP R/3*

The batch-input process is no longer necessary.

Within BW, the RFC (Remote Function Call) has a special significance because the data from the original system is transferred using this interface.

The PC download, which can be prevented using the authorization object S_GUI, is also still an option. The download option should also continue to be regarded in a differentiated way within the realm of the various reporting tools (see Chap 2.7). Since display in the BEx Analyzers generally is done via MS EXCEL, the contents displayed by each user can be saved on a local medium. This process cannot be caught with an authorization check. It behaves the same when the user can access the BW data using a Web browser. Only when the SAPGUI is being used, is the authorization object still valid.

Recommendation: Only allow access to BW using the BEx Analyzer or Web browser in only those cases and for users where the possibility of changing the reporting purpose does not have data protection implications or where it can be guaranteed – by other technical, organizational and qualification measures – that the data will be processed only with the framework of the existing legal foundation.

2.7.2.10 Auditing und Logging

In general, BW is a reporting tool that allows only the following restricted options for changing data:

- Loading information from the preloaded system
- Transformation
- Access on the table level.

As in R/3 classic, the configuration and reporting of logs and manual changes should be agreed upon with the data protection official.

Reference: Chapter 4.2.9 of the *Data Protection Guide for SAP R/3*

Within BW, AIS is currently not yet available because these components are linked with the existence of FI components. On the DSAG side, a development request has been made and acknowledged by SAP, to integrate the „System Audit“ part into the basis components.

The report logging within HR has no significance within BW. However, changes to system settings have to be logged analogous to R/3 classic. The same options are available for this with the security audit log, the system log and the transaction log STAD.

Beyond that, the data transfer logging process is defined using load logs. You can look at these logs using transaction RSMO.

2.7.2.11 Correlation of Data Protection Guides for R/3 - BW

Topic from Data Protection Guide	BW Guide
4.1 Requirements	2.7.1 Identical, thus only short introduction
4.2.1. Identification and authentication	2.7.2.1 Largely identical; enhanced with description of innovations regarding end user logon
4.2.2 Standard users	2.7.2.2 Identical
4.2.3 User authorization concept: selected authorization objects	2.7.2.3 Completely new where all of the new BW authorization objects are listed and under the transaction RSSM to create your own objects
	2.7.2.3 System rights are similar; only general differences are referenced
4.2.4 User authorization concept – selected profiles	2.7.2.4 New with a description of the profile generator / role concept 2.7.2.5 New: Example for expert design of the role concept within BW
4.2.5 Features of authorization check	2.7.2.6 Similar; RSSM as a new topic
4.2.6 User administration	2.7.2.7 Similar, enhancement with new authorization objects for user administration
4.2.7 Changes to productive system	2.7.2.8 Similar; description of options for changing data within BW
4.2.8 System interfaces	2.7.2.9 Enhanced with description of the basic differences
4.2.9 Auditing and Logging	2.7.2.10 Description of the differences (esp. no AIS;

Topic from Data Protection Guide	BW Guide	
	importance of load logs)	
4.2.10 Complex search help	Not a relevant BW topic	
4.2.11 Summary of main risks	3.1	Similar; enhances with notes on special risk fields
4.3 Summary of the audit activities	3.2	Audit activities were enhanced with BW-specific checks

3 Risks / Evaluation of Case Groups

When processing personal data in a data warehouse, special risks are to be considered regarding the personal rights of those affected, namely:

- The separation of the datasets from the operative processes, thus making these datasets independent.
- The option of combining data that is processed separately in the operative systems;
- The danger of wrongful use of the data;
- Processing outside of the legally permissible framework;
- Saving data without limitation of use, which is not the intent of legislators and is not allowed by the constitution ;
- Public administration may breach the constitutional ban on recording and saving of data for undetermined purposes;
- A change of purpose without providing the affected party with the option of assessing the textual and temporal consequences of the consent;
- Validity of the consent according to section 4a BDSG only upon the will of the affected party (this is contentious in a work relationship), declaration of purpose, note on consequences of refusal, in written form, if there are no special circumstances. (In data warehouse systems, the affected party is usually not aware of the purpose of the data and also what he is getting himself into)
- Circumvention of the imperative to make the affected parties aware of the change in purpose beforehand;
- A breach of the ban on data reduction and data economy (for example due to a lack of rendering data pseudonymous or anonymous, in both cases, the identification of people is not possible for the BW user);
- Circumvention of the legally defined period for retaining data;
- Via choosing to use BW to factually undermine the legally mandatory technical-organizational measures;
- The danger of not being able to sufficiently secure the legal requirements due to untested acceptance of technical proposals;
- Being unable to control a decrease in the level of protection;
- Endangerment of data protection targets based on the special complexity of data processing in business warehouses.

In addition to careful design of the business warehouse, these risks must also be counteracted with suitable technical-organizational measures and audit activities. Specific audit activities for BW can be found in chapter 3.2. More information on general audit activities for SAP R/3 can be found in chapter 4 of the *Data Protection Guide for SAP R/3* .

3.1 Summary of Main Risks

In general, the risks involved with using BW are almost identical to those that arise in using R/3 systems. Thus you can refer to the *Data Protection Guidelines for SAP R/3* (chapter 4.2.11).

Special risks also occur regarding permissibility of data processing: On the one hand, there is the risk that the data is processed for a purpose other than the one agreed upon (change of transformation rules), and on the other hand, that more individual data than previously determined is transferred to the BW (expansion of transfer rules).

3.2 Summary of Audit Activities

When checking the BW systems, in general, comparable audit activities as those used in R/3 systems are valid.

Reference: A comprehensive description of the audit activities can be found in Chapter 4.3 of the *Data Protection Guide for SAP R/3*. Features regarding BW systems are described in the following sections. We will stick to the established structure in the *Data Protection Guide for SAP R/3*, namely in the sections:

- Requirements for auditability
- As needed, special technical-organizational requirements from overriding laws, for example from company or employer agreements
- Data protection requirements according to section 9 BDSG and the appendix

3.2.1 Requirements for Auditability

Hardware
In addition to the aspects listed under 4.3.1.1 in the <i>Data Protection Guide for SAP R/3</i> , the following audit activities are significant:
Which source systems are used for the BW system? How is the data transfer from the source systems to the BW system realized from a hardware point of view?
Operating System and Low-Level Software
In addition to the aspects listed under 4.3.1.2 of the <i>Data Protection Guide for SAP R/3</i> , the following audit activities are significant:
- none-
Programming Technique
In addition to the aspects listed under 4.3.1.3 of the <i>Data Protection Guide for SAP R/3</i> , the following audit activities are significant:
Program development, program tests and test of customizing settings Are there binding directives regarding the use and procedures for programming

techniques?

- Web Programming
- XML Programming
- ABAP Dictionary / ABAP Workbench
- Data Modeler
- Business Object Repository
- Customer enhancements
- CATT Test cases (Computer Aided Test Tool)

Are the authorizations for programming in the BW development and production system designed and assigned correctly?

Run reports using transaction SUIM for the application-related authorization objects (e.g. S_DEVELOP, S_TABU_DIS, S_TABU_CLI, S_TABU_LIN, S_TRANSPRT, S_CTS_ADMI) and also for the authorization object S_TCODE e.g. regarding the following transactions:

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

Program documentation

Are programs and customer-defined objects documented in a comprehensible manner?

In addition to the transactions SA38 for monitoring the program documentation that can be defined on the system side and SE11 for table documentation, the following transactions are available:

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

3.2.2 Checking Special Regulations from Overriding Regulations

Appendix to User Authorizations

In addition to the aspects listed under 4.3.2 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant:

Are customer-defined BW authorization objects used in the BW system? Check this using the transaction SUIM and the selection for objects beginning with “S_RSR” and “Z”.

Do the determinations from the customer-defined authorization objects provide for the overviews via the user with access-authorization? Can the TARGET – and ACTUAL status of the users with access authorization be reconciled? For system-side checks, use the report RSUSR002.

Which source systems are used for the BW?

How is the data transfer from the source systems to the BW system realized – technically and organizationally?

3.2.3 Checking the data protection measures according to section 9 BDSG and appendix

Numeral 1: Access Control

No special measures for SAP BW systems.

Numeral 2: Access Control

In addition to the aspects listed under 4.3.3.2 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant:

How is access to the BW system regulated? Which processes (e.g. SAP Logon, Portal Excel-Plug-in) are used and is there sufficient secure identification of users?

Numeral 3: Access Control

In addition to the aspects listed under 4.3.3.3 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant:

Are customer-defined BW authorization objects being used? Evaluate this using transaction SUIM for this.

Are these customer-defined objects documented properly?

Is suitable access protection for personal data guaranteed using the corresponding roles or authorizations? Evaluate this using report RSUSR002.

Which users have the option of reading data directly from the PSA (Persistent Staging Area) and changing it there? The PSA is stored on the database using transparent tables. Thus you should evaluate the users with access authorization in regard to the following authorization objects:

- S_TABU_DIS – Table maintenance (especially client-independent tables)
- S_TCODE – Transaction code check (e.g. in regard to SE16, SE17, SQVI)

Further, you should analyze the users with access authorization in regard to the following function modules:

- RSSM_API_REQUEST_GET Link between InfoSource and requests
- RSAR_ODS_API_GET Read data records for the PSA table
- RSAR_ODS_API_PUT Write changed data records to the PSA table

Are the access rights properly designed in regard to administration of InfoSources and are they assigned to the users? InfoSources generally represent the basis for reporting. To do this, check the authorizations for the authorization

- S_RS_ISOUR Administrator Workbench – InfoSource.

It is very important that you evaluate specifications for the activity with the value 03 (display InfoSource data) and 23 (InfoSource transfer rules / maintain InfoSource data).

Which users are able to read or manipulate personal data in ODS objects? ODS objects (Operational Data-Store objects) are used to store cleaned up master and transaction data. On the database, the ODS objects such as PSA data are represented by transparent tables. Use these to check application and scope of ODS objects as well as users with access-authorization analogous to the access rights regarding the PSA.

Numeral 4: Transmission Control

In addition to the aspects listed under 4.3.3.4 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant:

If there is an overview/list of the locations at which program-controlled data transmissions could take place. In SAP BW, this includes, on the one hand, the systems that deliver to the BW system, and on the other hand, the systems that the BW system supplies.

Numeral 5: Input Control

In addition to the aspects listed under 4.3.3.5 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant:

The load logs should be checked carefully for compliance with the operation agreement (transaction RSMO).

Numeral 6: Job Control

In addition to the aspects listed under 4.3.3.6 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant:

None

Numeral 7: Availability Control

In addition to the aspects listed under 4.3.3.7 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant::

None

Numeral 8: Guarantee of Limitation of Use

In addition to the aspects listed under 4.3.3.8 of the *Data Protection Guide for SAP R/3*, the following audit activities are significant:

Is the assignment of users/functions/authorizations on the access protection level strict enough for the allowed purposes? Check the accessibility specifically for BW for users and individual user groups

- Business Explorer Analyzer (Transaction RRMX)
- BEx Monitor / Query Monitor (Transaction RSRT1)

4 References

- 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

- Administrator Workbench 8, 16, 17, 18, 19, 20, 21, 22, 32, 35, 41, 49, 55, 56, 57, 58, 59, 60, 63, 72, 73
- Aggregate 22, 57
- Aggregated Data 8
- Aliasing 11, 13, 37, 38
- Analyzer 75
- Archiving 27, 42
- ASAP 25, 28
- Audit Activities 69, 71
- auditability 71
- Authorization Concept 7, 10, 34, 48, 63, 64, 65
- BDSG 5
 - § 4a 70
 - § 4b, 4c 37
 - § 9 34, 71, 73
 - Section 28 (1) 14
 - section 4e 31
 - Section 9 27, 34, 54
- BDSG Section 3 (9) 34
- BEx Analyzer 44
- Browser 18, 45, 72
- Business Blueprint 25, 26
- Business Content 22, 25, 28, 29, 30, 35, 47, 50, 51, 53
- Business Explorer 8, 43, 45, 56, 60, 61, 62, 75
- BW Administration 64
- BW Statistics 32, 33, 35
- Change of Purpose 10
- Consent 10, 14, 70
- Contractual Data Processing 36
- Conversion Rules 20
- Customer Namespace 23
- Customizing 27, 65, 67, 71
- Data Basis 13
- Data Economy 9, 13, 27
- Data Format 17
- Data Mart Interface 33
- Data Model 26
- Data Protection Guide for SAP R/3* 31
- Data Protection Guide for SAP R/3 5, 10, 26, 31, 32, 34, 36, 37, 54, 55, 62, 64, 66, 67, 68, 70, 71, 73
- Data Protection Official 25
- Data protection officials 5
- Data Protection Official 25, 26, 30, 32
- Data Protection Official for SAP R/3* 32
- Data Reduction 9, 13, 27
- Data Retention 10
- Data Transfer 13, 26, 37, 64
- Data Warehouse 7, 9, 37, 70, 76
- Data Warehousing 7, 9, 39, 76
- DataSource 8, 16, 17, 21, 39, 41, 60
- Debugging Tool 62
- Deletion Terms 27
- De-Personalization 38, 42
- De-Personalizing 37
- Download Scheduler 47
- Eligibility Criterion 10
- EU Data Protection Directive 31
- EU Directive 54
- EU-Directive 5, 37
- Extraction Structure 16, 17, 41
- Extractor 16, 29
- Function Transfer 36
- Implementation Methods 25
- InfoCube 8, 21, 57, 63
- InfoObjects 8, 17, 18, 19, 20, 21, 22, 23, 29, 32, 33, 39, 63
- InfoPackages 21, 33
- InfoProvider 20, 21, 32, 61
- InfoSource 8, 18, 19, 20, 21, 39, 41, 59, 73
- Joining 8
- Legal foundation 10, 14, 26
- Limitation of Use 26, 70
- Limitation of Use for Specific Purposes 10, 14
- Limited Use 54
- Loading Logs 34
- Logging 68, 69
- Master Data 8, 18, 19, 20, 21, 22, 58, 62, 63
- Metadata 18, 19, 28, 36, 56, 59
- Metadata Repository 17, 18, 19, 20, 21, 22, 32, 35, 36
- ODS Object 13, 20
- Open Hub Service 33
- Operational Data Store
 - ODS 8, 19, 20
- Overviews 31
- Period for Retaining Records 32, 42
- Persistent Staging Area 8
- Personality Rights 9
- Possibilities of Analysis 13
- Preliminary Check 25, 31
- Prior Checking 11
- Productive Operation 28
- Project Planning 29
- Project Preparation* 25
- PSA 8, 13, 17, 18, 19, 63, 65, 67, 73
- Purpose 31
- Query 23, 61
- Query Designer 42, 44
- Query Monitor 35, 75
- recipient 26
- Recipient 31, 33, 34
- RemoteCube 8
- Reporting Methods 26, 27
- Reporting Options 26, 45, 65
- S_GUI 68
- SAP Data Protection Guide for SAP R/3* 66
- SAPGUI 68
- security guide 5
- Security Guide 26, 28

Sequential File	7	SE11	72
Solution Manager	25, 28, 30	SE16	63, 73
Source System	15, 16, 17, 26, 33, 65	SE17	73
Specific Circumstances	54	SE38	63, 72
Staging Area	17, 26, 65, 73	SE80	72
Star Schema	8, 22	SE95	72
Storage Time	10, 13	SM04	33
Supplier	11	SPRO	17
System Support	64	SQ07	72
Table Logging	67	SQVI	73
Technical and Organizational Measures	34	STAD	68
Technical-Organizational Measures	26, 32, 54	SU24	66
Third Country	37	SU25	66
Transaction		SU26	66
PFCG	55, 63, 66	SUIM	33
RS02	17	SW01	72
RSA1	16, 32, 33, 35, 72	SWO2	72
RSMO	35, 68	Transaction Data	8, 16, 18, 19, 20, 21, 73
RSRT	35	Transfer	26, 27
RSRT1	75	Transfer Rules	8, 20, 41, 59
RSRTRACE	62	Transfer Structure	16, 17, 19, 20, 21, 41
RSSM	56, 62, 66, 67, 69, 73	Transmission	32
SA38	72	Transparency	14, 31
SBIW	17	User Administration	64, 67
SD11	72	User Roles	26, 27
SE06	67	Web Application Designer	44, 47, 62
SE09	72	Works Agreement	10, 13

Glossary

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

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

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