Preface

The SAP ERP 6.0 Data Protection Guidelines manual has been written for data protection officials and others who have the responsibility to install and configure SAP applications in SAP ERP systems. Essential steps and points to consider are provided which assist in the implementation of SAP systems which are compliant with current data protection legislation.

This manual is meant to be a "recommendation", not an obligatory requirement or a standard. All responsibility for type, extent and results of the implementation of data protection regulations remains thus with the management of the responsible organization (enterprise/authority).

For the study of this manual basic knowledge of SAP systems, familiarity with commerce and tax regulations\(^1\), as well as with the German Federal Law for Data Protection (BDSG), are required. The manual addresses questions which are already contained in the SAP Security Guidelines or in other test manuals of the DSAG AK-Audit, particularly those questions related to data protection regulations. This version also deals with some module specific issues, such as those found in HCM (Human Resources).

In SAP ERP the classical ABAP world (ABAP stack) has been supplemented by the JAVA world (JAVA stack). This manual covers only the ABAP stack. The version for the JAVA stack is in the planning stage. SAP ERP itself is sold as standard software for an international market. The data protection recommendations in this manual are based on the European Union guideline 95/46/EG and the German Data Protection Act.

The authors are members of the DATA PROTECTION sub-group in the DSAG Audit Working Group and have written this manual based on their combined experience.

\(^1\) For example, HGB, AO, GDPdU, GoB/GoBS
CONTRIBUTORS TO THE 1ST AND/OR 2ND EDITION:

Mr. V. Ahrend  Bosch Telecom GmbH, Frankfurt
Mr. R. Anhorn  Robert Bosch GmbH, Stuttgart
Ms. C. Bonni  Lausitzer Braunkohle AG, Senftenberg
Mr. W. Kilian  RWE Energie Aktiengesellschaft, Essen
Mr. A. Lenz  Rheinbraun AG, Köln
Mr. S. Dierschke  BASF AG-Zok, Ludwigshafen
Mr. W. Geesmann  KPMG Deutsche Treuhand-Gesellschaft, Düsseldorf
Mr. R. Glagow  PWC Deutsche Revision AG, Düsseldorf
Mr. F. Glaß  PWC Deutsche Revision AG, Düsseldorf
Mr. T. Glauch  KPMG Deutsche Treuhand-Gesellschaft, Düsseldorf
Mr. J. Heck  Brau und Brunnen AG, Dortmund
Mr. G. Hohnhorst  KPMG Deutsche Treuhand-Gesellschaft, Düsseldorf
Mr. W. Hornberger  SAP AG, Walldorf
Mr. A. Kirk  Ruhrgas AG, Essen
Mr. K. Lorenz  Deutsche Bürgschaftskasse Badenia AG, Karlsruhe
Mr. Dr. Pötschat  BASF AG, Ludwigshafen
Mr. E. Schmidt  Philip Morris GmbH, München
Mr. A. von der Stein  RWE Systems AG, Dortmund
Mr. U. Ueberschar  Mannesmann Arcor AG & Co., Eschborn/Köln
Ms. G. Zibulski  SAP AG, Walldorf

The authors carry the responsibility for the contents of this document. The editorial work and layout are provided by SAP-AG and DSAG.

DISCLAIMER:
This publication is protected by copyright. All rights, unless expressly marked otherwise, are owned by:

Deutschsprachige SAP-Anwendergruppe e. V. (German-Speaking SAP User Group)
Altrottstraße 34a
69190 Walldorf
Germany

No unauthorised use whatsoever is permitted. This applies in particular for duplication, distribution, translation or use in electronic systems/digital media.
READER CONTRIBUTION / SUGGESTIONS FOR THE SAP ERP DATA PROTECTION GUIDELINES

My contribution/suggestion relates to the following topic(s)

( ) Critical tables/Customizing, Settings
( ) Critical objects
( ) Critical SAP facts
( ) Examples for concrete implementation measures and testing methods
( ) Other

I AM REFERRING TO...
SAP ERP Data Protection Guidelines, Chapter: ........................................................................................................................................................................
SAP ERP, Release: ..........................................................................................................................................................................................

MY CONTRIBUTION / SUGGESTION:

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

I AM PROVIDING ADDITIONAL INFORMATION IN AN ATTACHMENT (PLEASE CHECK YES OR NO):

( ) Yes
( ) No
1 INTRODUCTION: DATA PRIVACY AND SAP ERP
1.1 BDSG Requirements for SAP ERP
1.1.1 Collection, processing or use of personal data
1.1.2 Transfer of personal data
1.1.3 Retrieval procedures
1.1.4 Special appropriation
1.1.5 Processing by contractors (service providers)
1.1.6 Notification of the data subject
1.1.7 Rights of the data subject
1.1.8 Public demand for information
1.1.9 Obligation to notify authorities
1.1.10 Obligation to report loss of data
1.1.11 Data processing employees and confidentiality
1.1.12 Training
1.1.13 Data protection measures
1.1.14 Overview of BDSG sections 4e, 4g and 18 (§2)
1.1.15 Prior checking of the processing procedures

1.2 Role of the data protection officer in the implementation of SAP ERP
1.2.1 Data protection officer – member of the SAP project team
1.2.2 The data protection officer and project milestones
1.2.3 Information sources for the data protection officer

1.3 SAP Facts
1.3.1 Customizing and ASAP - Procedure Models
1.3.2 Authorization concept
1.3.3 Change Transport System / Change Transport Organizer (CTS / CTO)
1.3.4 Interface processing
1.3.4.1 Data transfer
1.3.4.2 PC Processing
1.3.4.3 Communication interfaces
1.3.4.4 SAP Automation
1.3.5 Job request procedure and job documentation

1.4 Risks
1.4.1 Absence of the data protection officer and/or the employee representative
1.4.2 Non-compliance with SAP recommendations
1.4.3 Omission or late implementation of the authorization concept
1.4.4 Improper use of data processing programs

1.5 Audit checklist for data protection implementation compliance

2 RESPONSIBILITIES OF THE DATA PROTECTION OFFICER
2.1 Monitoring the legal usage of data processing applications
2.1.1 Inclusion of the DPO in program development and system adjustments
2.1.2 Checking the legality of data acquisition and data use
2.1.3 Evaluation of logging
2.1.4 Examination of the procedure documentation
2.1.5 Issues related to the definition and auditing of the authorization concept
2.1.6 DPO Role in defining the operations concept and organization
2.1.7 Development of a data protection guide for users (Privacy Statement)
2.1.8 Monitoring of the Change & Transport System in SAP ERP

2.1.9 Routine and random checks of system operations

2.2 Special training for employees who work with personal data (§§ 4G and 5 BDSG)

2.2.1 Employee subgroups with data privacy obligations

2.2.2 Contents of the data privacy training for users

2.2.3 User training in the SAP system

2.2.3.1 User training for infotypes "COMPANY INSTRUCTIONS" or "QUALIFICATIONS"

2.2.3.2 User training for "TRAINING AND EVENT MANAGEMENT"

2.3 Management of the data protection documentation (BDSG Sections 4G-2, 18-2)

2.3.1 Information for the controller

2.3.2 Purposes of the data acquisition, processing or usage

2.3.3 Description of the data subject groups and relevant data or data categories

2.3.4 Recipients or categories of recipients

2.3.5 Deletion regulations

2.3.6 Planned transmission to third countries

2.3.7 Measures for the guarantee of security

2.3.8 Access authorized persons

2.3.9 Example registration form

2.4 System support

2.4.1 Evaluation of personal data in tables and fields

2.4.2 Techniques for finding personal data

2.4.3 Audit of the access authorizations

3 RIGHTS OF THE DATA SUBJECT AND OF THE GENERAL PUBLIC

3.1 Notification and information

3.1.1 Legal requirements

3.1.2 SAP Facts

3.1.3 Requirements for the organization of data protection

3.2 Correction, deletion and locking

3.2.1 Legal requirements

3.2.2 SAP Facts

3.2.3 Organizational requirements related to data protection

4 IMPLEMENTING THE REQUIREMENTS OF BDSG SECTION 9 AND ITS APPENDIX: TECHNICAL AND ORGANIZATIONAL MEASURES

4.1 Requirements

4.1.1 Statutory Requirements in Article 9 of the German Federal Data Protection Act

4.1.2 SAP Solutions for Compliance with the Statutory Requirements

4.2 SAP Facts, Risks, and Measures

4.2.1 ABAP Facts; Risks and Measures

4.2.1.1 Identification and Authentication

4.2.1.1.1 SAP Facts

4.2.1.1.2 Risks and Measures to be taken

4.2.1.2 Standard Users

4.2.1.2.1 SAP*

4.2.1.2.2 SAPCPIC

4.2.1.2.3 DDIC

4.2.1.2.4 EarlyWatch
6.3 SAP GRC (Governance, Risk and Compliance)

6.3.1 SAP GRC Access Control

6.3.1.1 Risk Analysis and Remediation (previously "Compliance Calibrator")

6.3.1.2 Enterprise Role Management (previously "Virsa Role Expert")

6.3.1.3 Superuser Privilege Management (previously "Virsa FireFighter for SAP")

6.3.1.4 Compliant User Provisioning (previously "Virsa Access Enforcer")

6.3.2 SAP GRC Process Control

7 SAP WEBSITES  

8 APPENDIX

8.1 Data Confidentiality Obligation – Form Letter  

8.2 Excerpt from the Federal Law for Data Protection

§ 5 Data Confidentiality  

§ 43 Administrative Offences  

§ 44 Criminal Offences  

8.3 Handling Personal Data – Recommendations for Employees  

8.4 Software Application Registration Form – (processing personal data)

8.5 Role of the Data Protection Officer in the ASAP Procedures Model  

8.6 Checklist of auditability requirements

8.6.1 Requirements for auditability

8.6.1.0 Is the JAVA stack active?  

8.6.1.1 Hardware  

8.6.1.2 Operating system and low-level software  

8.6.1.3 Programming techniques  

8.6.1.4 Additional check procedures

8.6.2 Check of special regulations which take precedence  

8.6.3 Additional check procedures

8.6.3.1 Item 1: Access control (Physical Access)  

8.6.3.2 Item 2: Access control (System Access)  

8.6.3.3 Item 3: Access control (Data Access)  

8.6.3.4 Item 4: Transfer Control  

8.6.3.5 Item 5: Input Control  

8.6.3.6 Item 6: Order Control  

8.6.3.7 Item 7: Availability Control  

8.6.3.8 Item 8: Data usage restrictions  

8.6.3.9 Miscellaneous checks
1 Introduction: Data privacy and SAP ERP

An SAP ERP installation specifically complies, in all its modules, with the requirements of the BDSG (German Federal Data Protection Act – see Sections 1, 12, and 27) with regard to automated handling of personal data by government organizations. This does not automatically apply to all data protection regulations for the Federal Republic and its Laender (states). Additional data protection regulations enacted by individual German Laender (states) are not referenced in this document.

This guide is appropriate for both public and private organizations.

Because SAP ERP has been designed as standard software for international business processes it can not be assumed by customers that every individual data field available is “compliant” with the German data protection regulations. Therefore, it is necessary that the (German) customer confirms that their SAP ERP installation meets all requirements of the BDSG, as well as local data protection regulations if they exist.

Both the data protection officer (DPO) and the works council or employee representative are therefore to be included in the project work. The responsibility for legally compliant implementation of SAP ERP lies with the organization’s project manager.

Although the BDSG mirrors the requirements of the harmonized EU data protection rights, the local exceptions and additions of the individual EU member countries and regions must be taken into consideration.

1.1 BDSG REQUIREMENTS FOR SAP ERP

The BDSG fundamentally prohibits the collection, processing, and use of personal data and only allows data processing of personal data when specific conditions defined in the BDSG are met. In order to incorporate this basic principle correctly in an SAP ERP installation, it is necessary to determine whether the BDSG requirements, and other regulations, have been appropriately implemented. The same principles and conditions apply to systems throughout their life-cycle.

1.1.1 COLLECTION, PROCESSING OR USE OF PERSONAL DATA

The collection, processing or use of personal data is expressly forbidden as described in section 4 of the BDSG, unless:
> the BDSG allows and/or demands the processing, or
> a regulation with higher precedence allows and/or requires the processing, or
> written consent from the data subject exists.

The admissibility criteria for the collection, processing or use of personal data are derived from section 4 BDSG with reference to:
> sections 13 and 14 BDSG for public bodies, and
> sections 28 through 32 BDSG for private and non-profit organizations.

The burden of proof for admissibility lies with the controller (controller).

The concepts of “data reduction” and “data economy” must be taken into account. These are defined in section 3a BDSG. Their general objectives are “to collect and use as little personal data as possible.”

The implementation of the data reduction and data economy principles in SAP ERP must incorporate the following points:

---

2 For the purposes of this document, the term “SAP ERP” includes the ABAP component and SAP NetWeaver.
> The regulations for collection, processing and use are each uniquely defined in the BDSG. The compliance for each concept must be individually examined and/or implemented (for example, with consent forms, service contracts, and/or staff/works council agreements).
> The organizational and technical measures for the use of SAP ERP are to be designed so that only the necessary personal data is stored. It should be noted that the SAP ERP software is delivered with standard (default) technical settings.
> With respect to a specific processing purpose, authorization concept decisions and other safeguards must guarantee that the data can be processed only WITHIN THE FRAMEWORK OF THE PERMISSIBLE PURPOSES. Data collected for different purposes must be processed separately using appropriate technical-organizational measures.
> Only the data needed to fulfil a task may be kept (DATA RETENTION PROHIBITION).
> Depending on the purpose of the data storage (for example, the fulfilment of a service contract), the necessary DATA FIELDS must be defined and entered in Customizing.
> In addition, the duration of data storage must be limited to a specific period of time and the deletion of the data guaranteed (for example, applicant data which is to be deleted at the end of a contract).

1.1.2 TRANSFER OF PERSONAL DATA
The transfer of personal data is generally forbidden. The admissibility criteria for transfers are specified in section 4b of BDSG with reference to sections 15, 16, 28, 29, 30 and 32. It is to be guaranteed that the limitations on use of the sent data are honoured by the receiver. This requires that the receiver be notified of these limitations (intended use).

For these reasons it must be confirmed that regularly scheduled or special-request data transfers are in compliance with data transfer regulations.

1.1.3 RETRIEVAL PROCEDURES
A retrieval procedure may only be established if the requirements of section 10 in the BDSG are met.
> In cases where personal data can be retrieved by a third party, additional measures to ensure the legal retrieval and secure handling of the data must be implemented by both organizations.
> In particular, the controller must ensure, by means of random sampling, that the transfer of personal data is legal.3

1.1.4 SPECIAL APPROPRIATION
In the event that personal data is saved as audit information in order to monitor data protection or security, or to ensure compliant operations (for example, log files or accounting information), this data may not be used for any other purpose (BDSG section 31).
> It must be determined which personal data can be used as audit information in SAP ERP, which SAP functions or organizations need this information and who will carry out the audit procedures.

1.1.5 PROCESSING BY CONTRACTORS (SERVICE PROVIDERS)
If personal data is collected, processed or used by a secondary organization (the service provider) by contract, the contractee (controller/principal) shall be responsible for compliance with section 11 BDSG and other regulations concerning data protection.

For details and exceptions; see Chapter 5.

3 The government draft of September 2007 provides additional requirements for random sample check procedures in section 29.
1.1.6 NOTIFICATION OF THE DATA SUBJECT
The data subject is to be informed about the collection and use of his personal data. Section 28b of BDSG requires that the notification be documented when address data is used in a credit rating score calculation. The notification can be waived only if the data subject is already aware of the legal circumstances.

In principle, the notification should take place when the data is collected from the data subject (for example, at the signing of a contract).

If the data is not collected from the data subject, but rather from a third party as in the purchase of addresses or transfer from a corporate affiliate, then section 33 of the BDSG requires notification if:
> this is the first time his personal data will be saved and/or transferred,
> his data has been collected by public bodies without his knowledge as defined in section 19a of the BDSG,
> his data will be saved and/or transferred by a private bodies for the first time as defined in section 33 of the BDSG.

If a notification is required, the notification procedure must be defined and documented.

1.1.7 RIGHTS OF THE DATA SUBJECT
Only permissible and correct personal data may be stored. Decisions which involve a legal consequence for, or have a significant impact on, the data subject must not be made exclusively on the basis of automated processing.

The data storage should be transparent to the data subject. This means the data subject has a right to information as well as to correction, deletion, blocking and objection. The requirements of section 6 of the BDSG in relation to sections 19, 20, 28b, 34 and 35 should be consulted.
> The controller must be in a position to reliably provide all of the pertinent details surrounding the collection of personal data to the data subject. This requirement refers to the “content of notification” discussed in section 4g, § 2, of the BDSG.
> An automated individual case decision is permissible, as described in section 6a of the BDSG, only in certain situations. If these exceptions occur, they are to be appropriately documented.

The requirements under which data blocking becomes necessary are to be defined. The use of blocked data must be regulated.

1.1.8 PUBLIC DEMAND FOR INFORMATION
According to section 4g §2 (sentence 2) the data protection officer (DPO) is obligated to provide the data collection overview described in 4e to any person upon request. If no DPO has been appointed, the responsibility lies with the company’s management.

1.1.9 MELDEPFLICHT
Section 4d of the BDSG requires that before automated processes are put into operation, the responsible regulators must be informed.
The obligation to notify can be waived per section 4d, §2, of BDSG if the controller has appointed a person responsible for data protection (a DPO). In this case, the DPO is responsible for providing the data collection details (“contents of notification”) as needed.

The obligation may also be waived if (a) personal data is collected, processed or used only for internal purposes and at most nine persons are employed for this purpose, and either (b) the data subject has given his/her consent, or (c) the collection, processing, and use of the data serve to fulfil a contract or similar agreement with the data subject.

1.1.10 OBLIGATION TO REPORT LOSS OF DATA
Among the requirements of BDSG section 42a are various obligations of supervisory authorities to inform data subjects in cases where certain categories of personal data were improperly obtained or distributed. This includes not only data stored in the SAP system, but all data extracted from, or in some way processed within the SAP system (for example, lists, office documents, e-mail attachments).

1.1.11 DATA PROCESSING EMPLOYEES AND CONFIDENTIALITY
The BDSG demands that all employees who deal with personal data must maintain confidentiality (data secrecy) as described in section 5 of the BDSG.

The duties related to confidentiality are to be documented for each employee.

Companies which are contracted to install or implement SAP ERP must inform their employees of their obligation to maintain confidentiality.

1.1.12 TRAINING
It is the responsibility of the data protection officer, per section 4g, §1 (2), to ensure that employees are familiar with data protection regulations from the BSDG or other sources, as well as rules derived from the data protection laws related to internal operations.

The data protection officer is also obligated to ensure that project participants and users who are involved in the installation and implementation of SAP ERP are informed of the BDSG requirements.

Records should be kept of the training provided.

1.1.13 DATA PROTECTION MEASURES
Personal data may only be collected, processed, or used if adequate technical and organizational data protection measure have been taken. The requirements for the individual objectives can be derived from section 9 of the BDSG and the BDSG appendix (extension of section 9).

Appropriate data security measures are to be taken and co-ordinated with the data protection officer.

If necessary the installed system can be subjected to an IT security audit for the improvement of data protection and data security.

1.1.14 OVERVIEW OF BDSG SECTIONS 4E, 4G AND 18 (§2)
The public bodies, according to the second section of the BDSG, must maintain a list of the data processing systems in operation as described in §2, and must document all the information referred to in section 4e of the BDSG, as well as the legal justification for the processing.
1 Introduction: Data privacy and SAP ERP

The responsible private and non-profit organizations referred to in section 3 of the BDSG must make available to the data protection officer an overview of the items listed in section 4e of the BDSG, as well as a list of persons with authorized access (see section 4g (§2) of the BDSG).

> The manner in which the required overview is to be created must be specified.

1.1.15 PRIOR CHECKING OF THE PROCESSING PROCEDURES

Independently of the obligation of the controller to involve the data protection officer in procedure implementations or changes, they must also implement an inspection of the automated processing procedures used to process sensitive data in order to determine whether a data privacy risk exists for the data subject. This sensitive data is described in sections 3 §9 and 4d §5 of the BDSG. The data protection officer is responsible for the prior checking. The prior checking procedure should be documented.

1.1.16 USING THE “SAP SOLUTION MANAGER” AS A SYSTEM IMPLEMENTATION SUPPORT TOOL

The SAP Solution Manager is the service and support platform of SAP which supports the introduction and implementation of SAP projects. If the Solution Manager is used, the persons responsible for data protection should make use of the documentation pertaining to system evaluation.

---

All business processes

All training course information

All test information

All information for service planning, Distribution and Follow-up

All change information

All service level information

All monitoring data

All customer developments and functional extensions

All information related to incidents and problems

The entire documentation

SAP SOLUTION MANAGER

---

1.2 ROLE OF THE DATA PROTECTION OFFICER IN THE IMPLEMENTATION OF SAP ERP

The BDSG section 4g §1.1 requires the early involvement of the Data protection officer in plans concerning the automated processing of personal data. This also applies to the implementation and software upgrades of SAP ERP.

> The data protection officer must be involved early in the project when SAP ERP is to be implemented in an enterprise.
> The data protection officer has the responsibility to determine whether both the Customizing and Implementation of SAP ERP meet the requirements of the BDSG.
> In particular, the principles of data reduction and data economy as described in section 3a of BDSG play an important role in the implementation of SAP ERP. This is an area where the data protection officer can directly impact the structure of the system.
> The data protection officer must also confirm that software upgrades are performed in compliance with data protection rules.

1.2.1 DATA PROTECTION OFFICER – MEMBER OF THE SAP PROJECT TEAM

The data protection officer has two important roles to play in any SAP ERP project – to provide professional advice to project leaders and team members, and to confirm that the installation (Customizing) is compliant with BDSG section 4g §1.1. The most effective arrangement is for the data protection officer to be a project team member.

If SAP ERP is being implemented in an enterprise, the data protection officer should be involved from the start of the project.

1.2.2 INFORMATION DES DATENSCHUTZBEAUFTRAGTEN ZU DEN „MEILENSTEINEN“

The responsibility to decide when and how the compliance of the SAP ERP system will be checked, and which materials are needed to accomplish that, lies with the data protection officer.

The decisions concerning which materials are needed and when the BDSG compliance checks will take place must be based on project objectives and development phases.

For each individual module (project milestone), the data protection officer should confirm with the project team that the agreed-upon implementation of the module complies with the requirements of the BDSG.

The data protection-relevant project steps are defined in the ASAP procedure model.

An example: ASAP procedure model (Roadmap)
2.6 Business process definition
2.6.3.1 Determine business process requirements
2.6.3.3 Determine report system requirements and co-ordinate with data protection officer
1.2.3 INFORMATION SOURCES FOR THE DATA PROTECTION OFFICER

The data protection officer should acquire an appropriate level of knowledge concerning the following elements of the SAP ERP system:

- The authorization concept and the profile generator.
- Table administration.
- The SAP programming language ABAP and ABAP Query (Advanced Business Application Programming).
- SAP ABAP Dictionary - All data fields of the SAP reference model are documented in the ABAP Dictionary. You can read an overview of the use of an individual field in the SAP environment using the "Where-used list" function.
- Procedures for the extraction and evaluation of data from SAP ERP with standard tools like Microsoft Excel, e.g.
- Help tools for the design and configuration of display screen templates (Screen & Menu Painter).

In order to provide reliable consulting and audit of the compliance of SAP ERP, the data protection officer also needs materials and information.

The following documents should generally be at the disposal of the data protection officer:

- The SAP Implementation Guide and the ASAP procedure model.
- The DSAG Guidelines from the AK Revision/AG Audit Roadmap SAP ERP 6.0 (from March 2009) found at http://www.dsag.de.
- SAP Security Guides provided by SAP. Refer to SAP Note 39267 for the availability of SAP Security Guides.
- The SAP Help (documentation CD), (http://www.sap.com/germany/aboutSAP/shop/)
- The SAP documentation in the internet (http://help.sap.com)
- Access to SAP Service Marketplace for the SAP Notes and additional information found at http://service.sap.com. (The data protection officer should review all documents with the keywords „data protection”, „data security”, and „security”.)
- IDES training system (IDES - Internet Demo and Evaluation System)
- Audit Information System. The audit information system (AIS) is designed to assist auditors and data protection officers with their work and is described in "Audit Information System" found in this document Chapter 6.1. The system audit and data protection sections in the current publication refer to SAP version R73 4.6c. Please see the SAP Note 77503 "Audit Information System."
- SAP Note 23611, "Security in SAP Products"
- SAP Note 30724, "Data Protection and Security in SAP Systems"

1.3 SAP FACTS

1.3.1 CUSTOMIZING AND ASAP - PROCEDURE MODELS

Customizing was divided into a transaction for project management (SPRO_ADMIN) and a transaction for project execution (SPRO).

The Customizing makes it possible to fit an SAP System to specific company needs. Due to the complex table structures of SAP ERP, SAP provides a system level Procedure Model and Implementation Guide
The correct implementation of SAP depends substantially on paying close attention to the SAP Implementation Guide (IMG).

The ASAP Procedure Model lists essential areas for which the data protection officer must determine, individually for each project, how he should be involved in project development.

Examples of tasks the data protection officer should be involved in:
- Define and document data protection-relevant business processes.
- Define master data.
- Define the report system.
- Examine the information flow of personal data with application interfaces, specifically data flows to other programs.
- Examine the information flow of planned reports and evaluate data protection criteria.
- Specify the data protection criteria for project milestone sign-offs.
- Evaluate the authorization concept sections related to data protection and data security criteria.
- Evaluate the archiving concept, in particular the deletion deadlines. (see chapter 2.3.5 Standard data retention periods)
- Evaluate the test plan.
- Specify data protection-specific training course contents and times.
- Specify documentation contents regarding data protection-relevant questions.
- Define migration and legacy data transfer.
- Assess and approve program customization.

The SAP Standard Procedure Model (Roadmap) and general notes for it can be found on the documentation CD or SAP Marketplace (http://service.sap.com). Recommendations regarding participation topics for the data protection officer related to the ASAP Procedure Model are located in Appendix 8.3.

The individual topics should be reviewed when planning the participation of the data protection officer and be used to determine the appropriate activities.

The SAP ERP Customizing Implementation Guide (IMG) can be found in the system menu path:
- Tools → Customizing → IMG → Project management (SAPADMIN), then the ‘SAP Reference IMG’ button

To see the customizing activities (Procedure Model) for a specific module in the Implementation Guide, find the appropriate Project Guide display.
Proceed as follows:

1. Call the project guide in the menu path:
   Tools → Customizing → IMG → Project management.
   Double-click a project, and then click the ‘Project IMG’ button.

2. Open activities sub-folders to reach the list of executable functions. Pick out the activities from the manuals that are relevant to data protection criteria, and identify the module-specific settings.

3. Contact the module-specific project groups and co-ordinate the necessary tasks.

### 1.3.2 AUTHORIZATION CONCEPT

With respect to data protection issues, an access protection system (with the option of assigning individual authorizations) has essentially the following goals:

> to protect confidential data from unauthorized collection, storage, reading and/or revealing, transmission and use;
> to protect the data from unauthorized, as well as inadvertent, change or deletion;
> to guarantee that the data is only used for specific purposes;
> to ensure that each data access of personal data is auditable and occurs only for specific permitted purposes.

SAP delivers a set of standard roles that the customer can use as a template to be customized as needed based on his business circumstances and organizational characteristics. The designs of standard roles are based on (employee) functions and must be modified to meet the security needs of the organization (segregation of duties, critical authorizations). An individual user menu is provided for each standard role. The standard roles are integrated components of the cross-application Workplace and Enterprise Portal /Portal Roles.

The start-up transaction SAP-Easy-Access provides the administrator with an expanded selection of functions. With this extensive list, the administrator can simply assign one of the many user roles to a user. When the user logs onto the system, he then has immediate access to the user menu applicable to his daily work, as well as the authorizations needed to complete this work.

The high flexibility of the SAP authorization concept and user administration concept, when carelessly used, can lead to significant problems for data protection even in the implementation phase. For this reason, the broadly defined standard roles and profiles are not appropriate and must be customized and restricted according to the “minimal authorization principle.”

Since the correct implementation of the SAP ERP system is affected directly by the authorization assignment procedure, the assignment procedure itself must be seen as an essential component of access protection. It must therefore be organizationally defined, easy to audit, thoroughly tested, and made available at the latest by the start of production.

And finally, it is important to ensure that roles and, when necessary, activity groups, authorizations and profiles are created, changed or deleted within the test/development system before being moved by the CTS/CTO (Change Transport System / Change Transport Organizer) into the quality assurance system and then, lastly, into the production system.
1.3.3 CHANGE TRANSPORT SYSTEM / CHANGE TRANSPORT ORGANIZER (CTS / CTO)

SAP recommends in general that no changes to the productive system are made or permitted. All changes are to be transferred from the test or quality assurance environment by the Change/Transport system to the productive system. A secure Change and Transport system is an essential component of a secure and compliant SAP ERP system.

With respect to data protection, the following objectives are of primary importance:

- the registration and documentation, as well as proper transfer, of system development environment objects (EUO) between the various SAP ERP systems or between various clients within an SAP ERP system;
- a guarantee that only authorized changes are made to the system and that those changes are clearly documented.

Due to the goals described above and the fact that EUO normally has system-wide validity, it is absolutely necessary that at least two, physically separated SAP ERP systems are implemented (test and productive system). If personal data from the productive environment (e.g. for mass tests of response time) in the test environment is used, anonymization or pseudonymization must be used.

If necessary, anonymization (identity masking) software tools can be purchased from third-parties. If this is not possible, other appropriate measures to ensure data security in the test system and test environment must be taken (time limits on authorizations for the test system, for example). The authorization concept applies to all systems, including development and test systems, especially if they contain personal data.

1.3.4 INTERFACE PROCESSING

1.3.4.1 DATA TRANSFER

SAP provides the LSMW (Legacy System Migration Workbench) as a data transfer procedure. This tool is designed particularly for the transfer of legacy data (data in an outdated format) and makes use of the BAPI (Business Application Programming Interface) - or batch input interface (see also LSMW transaction).

Because the data conversion from the legacy or feeder system is executed by programs outside the SAP ERP environment, it is necessary to guarantee a correct conversion (data consistency) by putting in place organizational measures to prevent possible data manipulation.

For data transfers in SAP ERP the Batch-Input-Procedure is also utilized. In this method an interface program creates a batch input session which simulates the online input of transaction codes and data. Authorization and plausibility tests are run during data input.

In addition to the Batch Input Procedure other data transfer methods exist such as Remote Function Call (RFC), Internet-interface or PC upload and download.

These are most often used for data transfers within the current enterprise (from front-end or back-end systems).

---

5 M. Schäfer, M. Melich: SAP Solution Manager, Galileo Press, Bonn 2006
6 See supplemental references in Chapter 6 – Auditing Test Guidelines
7 See supplemental references in the SAP Security Guidelines
1 Introduction: Data privacy and SAP ERP

All interfaces used for data transfers or data forwarding are to be documented as described in section 4e of the BDSG.

1.3.4.2 PC PROCESSING
Upload/download in applications (see also chapter section 4.2.1.8.3)

1.3.4.3 COMMUNICATION INTERFACES
The data-oriented interface Remote Function Call (RFC) enables SAP and non-SAP applications to call SAP function modules from computers outside the SAP system. Business-object methods can be called directly by Business Application Programming interfaces (BAPIs), which can themselves be called by external programs.

These business-process oriented standard interfaces are designed to work as dialog communications. They allow the SAP ERP core system to supplement its set of applications by running external programs developed especially for the internet or intranet.

BAPIs are handled like function modules in SAP ERP and can be called from RFC.

Application Link Enabling (ALE) makes the distribution of SAP ERP system data possible. Standard solutions are provided that describe how an enterprise can carry out and organize its geographical (multiple locations) data processing.

With ALE/WEB distributed business processes can be “outsourced” to business partners.

The ALE environment uses BAPIs for the integration of distributed business processes.

1.3.4.4 SAP AUTOMATION
This interface allows alternative user interfaces (GUIs) to be implemented instead of the SAP GUI. In addition to communication security, it must be determined whether personal data can be exchanged or transmitted via this interface, and who the usual recipients are.

1.3.5 JOB REQUEST PROCEDURE AND JOB DOCUMENTATION
In the relationship between data protection and the job request procedure; the most important concerns are the security and integrity of enterprise and personal data.

Jobs requests that require special handling which cannot be completed within the normal department processing, are especially vulnerable. These types of job requests must be official written requests. The requestor is normally a company department, such as Finance or Human Resources. Jobs that are generated by the SAP system are automatically documented. When jobs are generated by users themselves (e.g. batch input sessions) the user must manually generate the documentation. This documentation should always be in a standard, agreed-upon format. Jobs are not transferred from the test system to the production system using the Change and Transport system, but rather are created wholly in the productive system.
1.4 RISKS

The implementation of SAP ERP systems and/or projects also involves special risks (related to the SAP facts above) with respect to data protection.

Errors made during Customizing and the misuse or mishandling of the correction and transport functions can result in an inappropriate SAP implementation. In addition, the planned technical and organizational measures can be negatively impacted by mistakes in the creation of the access authorization concept.

1.4.1 ABSENCE OF THE DATA PROTECTION OFFICER AND/OR THE EMPLOYEE REPRESENTATIVE

If the data protection officer and/or the employee representative are not involved early on in the implementation as well as in subsequent modifications, the risk exists that data protection issues (such as prior checks of procedures, saving or transfer of inadmissible data) and the right to participate in project work decisions will not be taken into consideration.

1.4.2 NON-COMPLIANCE WITH SAP RECOMMENDATIONS

Disregarding SAP recommendations, particularly those in the SAP ERP Security Guidelines and SAP NetWeaver Security Guides (see http://help.sap.com), can result in an inappropriate and non-compliant system implementation.

Disregarding SAP recommendations can lead to the following risks:

> Possible access to the operating system, database and network levels;
> Inappropriate deviation from the Procedure Model and/or the implementation Guides (IMG) in Customizing;
> Insufficient documentation and explanation of the customizing settings;
> Insufficient interface documentation (batch input, PC download, necessary system expansions, archiving systems)

1.4.3 OMISSION OR LATE IMPLEMENTATION OF THE AUTHORIZATION CONCEPT

During the implementation phase of the SAP ERP, or of new components, a business/user authorization concept should be created. This concept serves as the foundation of, among other things, the structure of roles. Roles are in used to create, either manually or by means of the profile generator, user-specific authorization profiles.

The authorization concept must be used systematically and consistently. The current status and access rights of each user should be documented. During Customizing, the SAP defaults (for authorizations and initial parameters, et al) need to be restrictively changed. With an insufficient and/or delayed user authorization concept the danger exists that authorizations with excessive and unnecessary rights will be assigned to users.
1.4.4 IMPROPER USE OF DATA PROCESSING PROGRAMS

In order to operate a legally compliant SAP ERP operation (in Germany), it is necessary to abide by the restrictions of the BDSG. Some specific data protection risks to keep in mind during the implementation of an SAP ERP system are:

> Insufficient data modelling because a process compliance test run, as defined in section 3 §9 BDSG, is missing.
> Illegal and/or careless handling of original personal data in the test system;
> Missing confidentiality agreements and/or insufficient sensitivity training of team members and users;
> Insufficient documentation of the personal data. The data subject has a legal right to: obtain information about their data, correct the data, block or delete their data, and be notified of changes affecting their data.
> Neglect of the double-verification principle in the context of the CTS (Change and Transport System).
> Insufficient definition of the transport layers (integration, consolidation and/or recipient systems) in the TCENTRAL and TCEDELI tables within the CTS;
> Insufficient security for the Transport program (tp. and/or R3trans) as well as insufficient storage of Transport logs;
> Missing history of transmission of programs and/or tables into the productive environment;
> If the CTS is not deployed, or is set up incorrectly, unauthorized programs and/or objects could use or process personal data

The reduction of the risks listed above also serves to reduce the personal risks for the organization’s leadership (criminal charges, regulatory offences, and penalties as defined in BDSG sections 7, 8, 43 and 44).

1.5 AUDIT CHECKLIST FOR DATA PROTECTION IMPLEMENTATION COMPLIANCE

The following checklist has been provided to assist the Data Protection Office and project team members. It consists of essential questions, without claiming to be complete. It is recommended that the checklist be revised and expanded as needed for each individual project. For additional test procedures see Chapter 4.

The following questions are to be answered by the project management for each SAP ERP component (e.g. function module) implemented:

1. Which tasks should the SAP ERP components cover?
2. For which employee groups (job applicants, employees, family dependents of employees, customers, accounts payable, contract workers, etc.) is data to be saved?
3. Which business processes are included?
4. Are data protection regulations taken into account early in the SAP project planning?
5. Were appropriate documents, particularly for preliminary data checking, made available to the data protection officer early in the project?
6. Is the data protection officer appropriately involved in the project work?
7. Which personal data is to be stored?
8. Which personal data is to be transferred to external organizations, and under which circumstances (regularly scheduled or by request)? Do external organizations receiving the data outside the European Union have equivalent data protection regulations?
9 Do the basic legal forms for collection, processing and use of personal data exist (contracts, consent forms, employment agreements, etc.)?

10 Is automated retrieval of personal data a requirement? If so, how will the security requirements for legally compliant data retrieval be implemented?

11 Are automated individual case decisions made? If so, are the requirements from section 6a, §2 applied?

12 Which interfaces with other data processing applications exist?

13 Which log files are planned and how will they be used (e.g. report log file in SAP ERP HCM, table V_T599R and creation of the security audit logs)?

14 How are the data usage restrictions described in BDSG section 31 handled?

15 Which data storage time periods are planned for the individual data sets with respect to the individual legal requirements?

16 What is the data deletion plan?

17 How is it guaranteed that access to data stored due to data retention laws (for example, data kept 10 years for tax reasons) is appropriately restricted?

18 Does the necessity exist to inform data subjects (persons)? If so, what is the notification procedure and which forms are used?

19 How is the security concept structured?

20 Are authorizations granted based on the minimal authorization principle?

21 Have the SAP security guidelines been followed and implemented?

22 Is encrypted personal data transmitted (this is possible for the SNC connection with SAPGUI and SAPLPD; RFC connections can be secured) and/or saved (this is a function of the database, not SAPERP)?

23 On which hardware and at which locations is SAP ERP to be installed?

24 Which data processing network is to be used?

25 Are adequate firewall systems installed for internet and intranet operations?

26 Is there written documentation describing all installed systems used for SAP ERP data processing?

27 If yes, how will the organization provide an overview to the data protection officer?

28 Will a procedures handbook be made available to the data protection officer?

29 Which organizational solutions are planned?

30 Are all recently added tables, domains, data fields and reports appropriately documented and sufficiently protected?

31 Are all persons with access to personal data also legally obligated to maintain confidentiality?

32 Will the data protection officer be notified before system upgrades and new software release installations occur?

33 Are there critical selection fields in reference tables or search functions which contain sensitive data such as religion (in Infotype 0002), marital status or number of children?
2 Responsibilities of the Data Protection Officer

Because the DPO (Data Protection Officer) is in most cases not a SAP specialist, he or she will work together with various employees within the organization. In the course of his activities he will interact with both users in various business departments and with IT employees. At times it may also be necessary to work with other units within the organization (such as internal auditing, i.e.) as needed to resolve specific issues.

The DPO needs adequate training in the use of the relevant SAP ERP functions in order to successfully carry out process compliance test runs, company customizing, and appropriate system testing.

SAP ERP is delivered with several auditor roles which are designed for the various function areas of the AIS (Audit Information Systems). These standard roles are merely templates for the organization-specific roles in the respective user operations and must be adapted to the operational structure and characteristics. The AIS standard roles are divided into transaction roles (which define the user menu) and authorization roles (which contain the authorizations).\(^8\)

Below is a table showing some of the SAP standard roles that are relevant for the DPO.

<table>
<thead>
<tr>
<th>ROLE</th>
<th>FUNCTIONAL AREA</th>
<th>SERVICE PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_AUDITOR_A</td>
<td>AIS Central Authorizations</td>
<td>The authorizations of the role are essential for business and data protection audits</td>
</tr>
<tr>
<td>SAP_AUDITOR_ADMIN</td>
<td>AIS Administration</td>
<td>This role contains functions for AIS administration</td>
</tr>
<tr>
<td>SAP_AUDITOR_DS</td>
<td>AIS Data Protection</td>
<td>The role menu contains the file tab for personal data</td>
</tr>
<tr>
<td>SAP_AUDITOR_DS_A</td>
<td>AIS-Data Protection (Authorizations)</td>
<td>The role contains authorizations for the data protection audit</td>
</tr>
<tr>
<td>SAP_AUDITOR_BA_HR</td>
<td>AIS Human Resources</td>
<td>The role menu offers functions for the business audit (individual financial statements) and for Human Resources (HR / HCM)</td>
</tr>
<tr>
<td>SAP_AUDITOR_SA</td>
<td>AIS System Audit</td>
<td>The role menu contains functions for the System Audit, especially system configuration, SAP system group, development, and Customizing</td>
</tr>
<tr>
<td>SAP_CA_AUDITOR_SYSTEM_DISPLAY</td>
<td>AIS Authorizations for System Audit (Display)</td>
<td>The authorizations for this role allow access to the System Audit (Caution: contrary to the SAP documentation there is no read-only right)</td>
</tr>
<tr>
<td>SAP_AUDITOR_SA_CCM_USR</td>
<td>AIS System Audit (User and Authorizations)</td>
<td>The role menu provides functions for user administration: users, authorizations, profiles, and roles</td>
</tr>
</tbody>
</table>

\(^8\) See also SAP Notes 754273 and 451960
Use the following SAP path to find the roles:

Menüpfad:
Tools → Administration → User Maintenance → Role Administration → PFCG – Roles

The SAP auditor roles are specifically defined for individual AIS functions. The SAP_AUDITOR_DS role initially contains only the AIS functions for the “File Register”. A combination with other roles (for example, SAP_AUDITOR_DS_A, SAP_AUDITOR_A, SAP_AUDITOR_HR or SAP_CA_AUDITOR_SYSTEM_DISPLAY) is the minimum needed to support the SAP audit activities of the DPO.

The roles delivered by SAP must be analyzed carefully and adapted appropriately to the enterprise. The narrowly defined data protection role “SAP_AUDITOR_DS” offers only the AIS overview menu option “File Register”. The role SAP_CA_AUDITOR_SYSTEM_DISPLAY contains critical authorizations including, but not limited to, read-only rights.

It is recommended that the SAP auditor role be customized to fit the organization. Through the audit information system (see Chapter 6) the DPO has sufficient read rights to conduct a system audit pertaining to data protection. This includes direct calls to the appropriate transactions and reports, but does not include access to employee personal data.

In addition, a second role can be assigned to the DPO which is designed specifically around the circumstances for testing real data. This second role can be granted for limited time periods as needed.

The certificate for “Development of Data Protection Roles for the Audit Information System in SAP ERP” covers the topics (a) evaluation of the SAP standard roles, (b) new concepts for data protection roles (for example, a role with read-only rights) and (c) review of features and characteristics.9

2.1 MONITORING THE LEGAL USAGE OF DATA PROCESSING APPLICATIONS

“The data protection official shall work towards ensuring compliance with this Act and other data protection provisions. …In particular, he shall…monitor the proper use of data processing programs with the aid of which personal data are to be processed;”

The following points are of special relevance:
> Validity of data processing concerning the principle of data reduction and data economy (§ 3a BDSG),
> Guaranteed protection of the data subject’s rights (§ 6 in connection with §§19 FF and/or §§ 34 FF BDSG),
> Obligation to maintain data confidentiality (§ 5 BDSG),
> Special technical-organizational precautions to maintain data protection. If special risks exist for the rights of the data subject, a process compliance test run is absolutely necessary (§ 4d exp. 5 BDSG).
> Employee data protection (Section 32 BDSG)

The following duties of the DPO, concerning the implementation of an SAP ERP system, can be derived from this regulation.

9 Otto, Anna: Entwicklung von Datenschutzrollen für das AIS im SAP ERP, VDM Verlag, Saarbrücken 2008
Download the data protection roles (in German) at http://www.forbit.de/allgemein/arbeitspapiere.html
2 Responsibilities of the Data Protection Officer

2.1.1 INCLUSION OF THE DPO IN PROGRAM DEVELOPMENT AND SYSTEM ADJUSTMENTS
The tasks of the DPO include both the protection of personal data as well as the security of the overall system. To make this possible, it is necessary that the DPO be involved from the beginning of development projects as part of the project management team. In addition, the DPO needs to be aware of program modifications and program interfaces. Test procedures are to be co-ordinated with other system managers.

Once the authorization concept is complete the testing of data protection relevant aspects and the defining of corresponding objects to be used can begin.

The data processing concept based on the authorization concept should include a section about personal data. Additional information about tables, field names, and data elements, as well as their use in programs is found in the ABAP Dictionary (transaction SE12) and in the Repository Infosystem (Object Navigator, transaction SE84). For additional system support information see chapter 2.4.

2.1.2 CHECKING THE LEGALITY OF DATA ACQUISITION AND DATA USE
The monitoring activities of the DPO are not limited to data processing (§ 3 of section 4 in BDSG). Monitoring also extends to data collection (§3 section 3 BDSG) and the use of personal data (§3 section 5 BDSG). This means that the validity of the data processing programs in place must be tested.

2.1.3 EVALUATION OF LOGGING
Several logs are available in SAP ERP. These logs can be used for various purposes and are described in detail in the SAP Security Guide.

The DPO should have access to logs which can be used to check and confirm that system operations are in compliance. The most important logs are listed below. (Note: An overview of the essential log entries can be viewed with the Audit Information System (System Audit, System Log, and Status Display). Details can be found in chapter 4.2.1.9.

> the Security Audit Log, Transaction SM20N (Filter setting SM19)
> System log Syslog, SM21
> the Work load monitor of the CCMS with Transaction STAD and ST03N
> in the Application log (Transactions SLG0 and SLG1)
> Business Workflow (Transactions SWI2_* and SWI5)
> Changes to business objects (Transaction SCDO)
> Customizing-Objects and table records (Transaction SCU3; Reports RSTBHIST and RS VTPROT)
> SQL-Audit (see also SAP Notes 115224)
> SAP Query Logging (see section 4.2.1.9.6)
> Log of Report starts HCM, Report RPUPROTD
> Change document HCM-Infotypes, Report RPUAUD 00
> Input log customer data (such as Batch Input Log, Job Log)

2.1.4 EXAMINATION OF THE PROCEDURE DOCUMENTATION
Comprehensive documentation of the procedures for monitoring software application usage must be available to the DPO. The following points must be covered:
> Scope of tasks in the application (i.e. restrictions), in particular with respect to data protection-relevant elements
> Technical-organizational measures in agreement with § 9 BDSG and/or the organization
> Access authorizations according to kind and extent of personal objects (such as data, programs, reports)
> Where-used list for the personal objects in programs
> Authorized internal and external recipients of the data, both type and extent, produced by the application programs.
> Representation of the program flows. Protection of the databases and the executed programs
> Deletion and locking concept as well as archiving (limitation of operational usage and “storage usage”)

SAP provides assistance related to the procedures documentation. Within the Audit Information System the RSCRDOMA report can be used, for example, to analyze personal domains via “File register functionality”. Detailed references to additional system functions can be found in section 2.3.3 and 2.4, among others.

2.1.5 ISSUES RELATED TO THE DEFINITION AND AUDITING OF THE AUTHORIZATION CONCEPT

The DPO is strongly advised to participate in the development of an organizational framework for the authorization concept. This early participation can help reduce the effort required for the process compliance test runs.

The authorization framework concept must address the following issues:
> the scope/territory (of the controller(s))
> the basic conditions; among other things the responsibility for maintenance and servicing of the SAP system including definition of the customizing tasks and their required authorizations (XE); rules for the change of system objects, particularly Repository objects (change, test and release procedures including the transfer into production)
> the technical–organizational configuration of the role-specific concept
  > possible job-related individual configurations for justified exceptional cases
  > functional structure
  > Principle of minimal and/or adequate authorization assignment
  > Transparency in the sense of the BDSG and auditability
  > Implementation of the requirements for restricted use (§ 31 BDSG) and data protection in the sense of § 9 BDSG and its operations
> the system-oriented configuration
> Principles for the use of the central user administration
> Handling of standard roles and profiles (Note: Do not use standard (delivered) profiles)
> Definition of restrictions of individual authorizations (Note: Consider all relevant systems and clients)
> Implementation of the pertinent organizational concept
> Separation of critical and non-critical transactions
> the requirements for an appropriate mapping, based on the restricted-use principle, of the enterprise organization(s) at the SAP structure/organizational level of systems, clients, accounting areas, works, areas of staff, etc.
  > a procedure for the classification and maintenance of authorization groups for ABAP reports and tables
2 Responsibilities of the Data Protection Officer

- the naming conventions; rules for the naming of user master records (no names without reference to a person), user groups, roles as well as other relevant SAP objects (including description of justified exceptions); naming rules for different roles such as read roles, roles with access to certain organizational units, transaction roles, etc.
- the establishment of emergency users
- the definition of authorizations for external users and their control
- handling special users such as SAP*, DDIC, SAPCPIC, and EarlyWatch
- the structure of the documentation; among other things clear responsibilities for updating the concept as needed for organizational-functional adaptations
- conventions for non-production systems which contain test data with real data or important documentation components which contain legal evidence
- rules for the assignment of profiles (without Profile Generator)

The following best-practices are recommended:

- The individual departments are responsible for the security of their data and thus also for effective access protection. Routine checks of the suitability of the assigned authorizations are to be carried out by the person responsible for the data.
- The user administration should be advised of user authorization changes as soon as possible.
- The administration of the authorization procedure should be distributed across several positions, organizational units or employees, and should be appropriately documented (separation of duties between creation, assignment and checking/auditing).
- The granting of user IDs must follow a clear procedure (authorizations in the system are granted only with written permission from the responsible person), and the validity of the user ID must be confirmed in a timely manner.
- Based on the technical role concept, users may only have the authorizations which are absolutely necessary for the completion of their tasks.
- The authorizations of privileged users should be both technically and temporally limited (see chapter 4.2). Emergency users should only be activated in emergency situations, and their use should be logged either through the Security Audit Log (SM20) or a similar tool.
- For non-employees and contract workers, as well as for remote support, the rights and time limits must be appropriately restricted (see SAP NetWeaver Security Manual).
- Application-oriented authorizations for developers are to be limited primarily to the development system.

In order to examine existing authorization concepts and to define, in particular, rules for the assignment of critical authorizations, SAP solutions such as the Audit Information System or GRC ACCESS control can be used (for details see chapter 6).

2.1.6 DPO ROLE IN DEFINING THE OPERATIONS CONCEPT AND ORGANIZATION
The DPO should be involved in the development of an organizational framework for the configuration of the operations concept from the beginning. The operations concept includes the basic structure of the SAP system on one or more servers, and with respect to the communications configuration, the network, operating system, and database management.
In addition, the DPO should provide timely recommendations concerning security standards needed at various levels to prevent manipulation and unjustified access to personal data.

Other recommendations for selected system and profile parameters are also a part of the DPO participation in the definition of security management, i.e. the process definition for security and data protection requirements.

A detailed description of the relevant topics is found in the SAP Security Guide. Among others, the following points are discussed:

- The only user of the database is the SAP system.
- It must be ensured that the layers beneath the database can not be accessed (by the database itself or the operating system). If not, the SAP authorization protection can be circumvented.
- Only a strictly limited circle of administrators have access to database tables and SAP data at the operations system level.

It is generally necessary to have an operator organization (responsible specifically for the administration of the SAP ERP system). The group may include several individuals if several enterprises/organizations are processed in one system.

The operator’s group can be centralized or decentralized, or a combination of both alternatives.

- The advantages of a decentralized operator organisation include the proximity to users and the flexibility of operator assignments within the enterprise, as well as the assurance of coordinated workflows. On the other hand, more agreements must be reached concerning inter-company activities and operations, and more manpower is needed.
- With a centralized administration it is possible to control specific areas of competence with a clear organizational structure, as well as make faster decisions when conflicts appear. Of course, some of the flexibility is lost concerning the corporate units processed within the SAP system, and it becomes more difficult to configure company specific requirements with shared configurations. It is also more difficult to prevent conflicts of interest within the management of the operator’s organization.

The DPO should be particularly careful to ensure that the demands of data protection of personal data, both confidentiality and security, are met with respect to the operator organization.

2.1.7 DEVELOPMENT OF A DATA PROTECTION GUIDE FOR USERS (PRIVACY STATEMENT)

When third-parties have been given internet access to the SAP system, the DPO should participate in the creation of a data protection document pertaining to the affected business processes.

In cases where these users do not already have the information, they should be informed of the type, extent and purposes of the collection and use of personal data and processing before gaining access.

This guide for users is meant as a service to business partners (third-party users) and should be delivered in a clearly understandable form with regard to the protection of the user’s privacy (confidentiality, integrity, and authenticity). Assistance with generating a privacy statement is provided by the OECD Privacy Statement Generator found at http://www.oecd.org/sti/privacygenerator
2 Responsibilities of the Data Protection Officer

2.1.8 MONITORING OF THE CHANGE & TRANSPORT SYSTEM IN SAP ERP

In order to protect the integrity and availability of the production system, it is necessary to divide the configuration into separate systems. For security reasons, a minimum of three systems are recommended: development, integration and production. The three systems are connected by the Change & Transport system. A description of effective protective measures can be found in the SAP Security Manuals.

One of the examples describes how to avoid the prohibited smuggling of programs or data into the production system via the SAP ERP Transport system. The solution requires a separation of the test system from the development system. It is recommended that the production system application and database computers are maintained separately from the SAP ERP application and use their own Transport system on the network side.

The DPO must therefore consider whether, or how, personal data could be transported into non-production systems, as well as how user and authorization values from front-end systems can land in the production system without examination of their content.

Note: Not to be forgotten is the specification of a disposal concept for test and/or no longer needed production system output or storage media (e.g. print-outs, hard-drives).

2.1.9 ROUTINE AND RANDOM CHECKS OF SYSTEM OPERATIONS

In addition to the monitoring tasks of the DPO both routine and random checks are needed of system operations organization and flow, the required segregation of duties, and the implementation of the access authorization concept. The log files also need to be evaluated. Additional information regarding the Security Audit Log and Audit Information System authorizations needed by the DPO to perform these tasks can be found in chapter 4.2.1.9.1 and chapter 6.

2.2 SPECIAL TRAINING FOR EMPLOYEES WHO WORK WITH PERSONAL DATA

2.2.1 EMPLOYEE SUBGROUPS WITH DATA PRIVACY OBLIGATIONS

Employees who collect, process, or use personal data in their work are obligated to maintain data privacy (§ 5 BDSG). The responsible organization is required to provide appropriate training (§ 4g exp. 1 No. 2 BDSG) to these employees.

The data privacy obligation generally applies to the following employee subgroups:
> Employees in all departments where PCs are in use
> Employees in computing centers, IT employees
> Employees in corporate departments which handle personal data, such as:
  > Personnel - wage and salary statements, time management
  > Sales, Marketing, and Advertising
  > Purchasing
  > Controlling
  > Messenger Services
  > Project team members
The data privacy obligation extends also to part-time workers and student interns. Union shop officials are also included in § 5 BDSG.

Employees of outside firms, e.g. external consultants, who have access to personal data, must also abide by the data privacy rules. The data protection officer cannot personally enforce this obligation on non-employees, but should include it in contracts and periodically check for compliance.

2.2.2 CONTENTS OF THE DATA PRIVACY TRAINING FOR USERS

The training should familiarize the user with the regulations of the BDSG as well as any data protection regulations pertinent to their specialized tasks. In addition, the users should be given general information about data protection laws and related references, especially for data security and data processing compliance. The goal of the training is to provide the users with the knowledge to perform their work within the data protection guidelines.

For training purposes PC training applications can be used. This training does not replace the responsibilities of the data protection officer, but can serve to enhance the user’s understanding of the material.

After successfully completing the data privacy training, the participants are to sign a corporate confidentiality agreement. A signed copy of this document (see BDSG, appendix 8.1) should be put in the participants personnel file. It is recommended that each training participant be given a copy of excerpts from the BDSG which apply specifically to their job as well as a summary of guidelines for working with personal data (appendix 8.2).

Another example of useful information for the participants can be seen in SAP Note 35493 – Secrecy and Data Security Obligations.

2.2.3 USER TRAINING IN THE SAP SYSTEM

2.2.3.1 USER TRAINING FOR INFOTYPES “COMPANY INSTRUCTIONS” OR “QUALIFICATIONS”

Users with access to mySAP Human Resources have the option of installing the data privacy training materials in the personnel master records in the SAP ERP system. The training course can be installed as follows by either the DPO or the personnel department:

- **Menu path:**
  
  Human Resources → Personnel Management → Administration → HR Master Data → PA30 Maintain

Either the Infotype 0035 (Company Instructions) or Qualifications (use Infotype 0024) in the employee profile in Personnel Development can be used. For the latter option The PLOG1 APRA switch in the Customizing table T77so must be set to 1.

The Qualifications Infotype refers back to the Qualifications Catalog. Thus, in terms of Customizing, the user training must be admitted into the catalog.
2 Responsibilities of the Data Protection Officer

Menu path:
Human Resources → Personnel Management → Personnel Development → Settings → Current Settings → Edit Qualifications Catalog (OOAQ)

The qualification catalog has a tree structure. The data protection training can be placed under the branch „legal fundamentals“, for example.

The report RHSTRU00 is used to execute the structure evaluation of the qualification catalog.

Using the report RXHQALIF (Attendee’s Qualifications) it is easy to review who is obligated to participate and which course has been completed. It is also possible to view information at the organization unit level. A comparison between employees in one department (such as Personnel or IT) and all obligated persons will reveal discrepancies. Special attention should be paid to new or transferred employees.

Recommendation: Organizations which do not use Human Resources – Organizational Management and Personnel Development should use Infotype 0035 (Company Instructions). All others can use Qualifications in the employee profile as described above.

2.2.3.2 USER TRAINING FOR “TRAINING AND EVENT MANAGEMENT”
For organizations which use “Training and Event Management” it is recommended that all user training be organized via this tool.

The Training and Event Management function can be used to plan, execute and manage events. This makes it convenient to schedule course participants, time and place, and course instructors, as well as determine working hours required.

2.3 MANAGEMENT OF THE DATA PROTECTION DOCUMENTATION (BDSG SECTIONS 4G-2, 18-2)
In the Customizing phase the data to be collected and saved is determined. During this phase the Data Protection Officer actively participates in the implementation of the data protection legal requirements.

In order to effective perform his tasks, the DPO requires (per §§ 4e and 4g Abs. 2 of the BDSG) the following documentation:

§ 4G PART 2 – DUTIES OF THE DATA PROTECTION OFFICIAL
“The controller shall provide the data protection official with an overview of the information stipulated in the first sentence of Section 4e and a list of persons entitled to access. The data protection official shall, on request, make the information pursuant to Nos. 1 to 8 of the first sentence of Section 4e available to anyone in an appropriate manner.”

§ 4E CONTENTS OF THE OBLIGATORY REGISTRATION
In so far as automated processing procedures are subject to obligatory registration, the following information is to be furnished:
1 Name or title of the controller (responsible organization)
2 owners, managing boards, managing directors or other lawfully or constitutionally appointed managers and the person placed in charge of data processing,
3 address of the controller,
4 purposes of collecting, processing or using data,
5 a description of the groups of data subjects and the associated data or categories of data,
6 recipients or categories of recipients to whom the data may be transferred,
7 standard periods for the erasure of data,
8 any planned data transfer into third states,
9 a general description which can be used to assess whether the measures implemented to protect processed data are sufficient (in accordance with Section 9 of the BDSG).

The information to be provided by public-bodies is essentially the same (see Section 18, #2), but with the additional legal requirement of written documentation.

§ 18, IMPLEMENTATION OF DATA PROTECTION IN THE FEDERAL ADMINISTRATION
“(2) Public bodies shall keep a register of the data processing systems used. In respect of their automated processing operations, they shall record the information in accordance with Section 4e and the legal basis for processing in writing. This requirement can be waived in the case of automated processing operations for administrative purposes which involve no restrictions of the data subject’s right of access in accordance with Section 19 (3) or (4). The specifications may be combined for automated processing operations which are conducted several times in the same manner or a similar manner.”

Because of the nearly identical requirements for the public and private sectors, the following remarks focus only on the responsibilities of the DPO as seen in BSDG Section 4G.

It should be noted that the same topic is included, nearly word-for-word, in the European Union guideline 95 / 46 / EG (Section IX, Paragraph 18 ff).

If the DPO wishes to take advantage of IT security resources to fulfil the responsibilities referred to above, he has recourse, if needed, to the IT security management audit of the enterprise in the context of the ISO-Norm-27001. This audit stipulates that, among other things, a survey of the IT systems and a list of IT applications (software, application programs, business processes) as well as additional instructions (for responsible administrators, personal data) must be completed. This forms the foundation of the internal operations procedures documentation.

RESPONSIBILITIES
In the amendments to the NDSG in 2001 the division of responsibilities between the data processing department and the DPO were adapted to better reflect current use: the “controller of the filing system” was renamed to “controller.” In addition it became the responsibility of the DPO to ensure that the organization moved towards observing the laws and regulation of data protection (BSDG, Section 4g-1-1). The following applies to all employees, but especially for data processing managers:
2 Responsibilities of the Data Protection Officer

The system operators (persons responsible for applications and systems) are responsible for the adherence to the laws and regulations related to data protection and data backup. The controller must adopt, among other things, measures that ensure that the data:

> is always processed legally and for specific purposes,
> is essentially correct and current,
> is stored only as long as needed for the specified purpose,
> is protected from un-permitted access and manipulation,
> is not distributed to third-parties without prior agreement.

In addition, each individual employee is responsible to ensure that the personal data entrusted to him is processed and used only within the scope of his job tasks. Each abuse or inadmissible passing on of this data is forbidden and can result in both consequences pertaining to labour law and may constitute a statutory offence.

It is recommended that these points are clarified by the responsible persons in the data protection documentation.

FORM OF THE DOCUMENTATION

While the contents of the documentation are described in detail in BDSG, Sections 4e and 4g, the form of the documentation is not specified. For the SAP ERP system a combination of written documentation (e.g. file notes, memoranda) and references to the electronic documentation (e.g. ABAP Dictionary, AIS) is sensible.

To meet these requirements, the dynamics of the SAP system can be used and individual details collected if they are needed. The minimum contents required by law must, however, always be kept up-to-date.

In the core of the documentation are the registration data as described in BDSG, Section 4e, supplemented by a list of persons with data access rights.

The controller must provide to the DPO the appropriate information for:

> Data for the contents of the registration obligation described in BDSG, Section 4e,
> The information described in BSDG, Section 4g-2 (1-8) must be made available to the general public upon request,
> The process compliance test run is to be executed for special risks after receipt of the documentation,
> The DPO needs the documentation in order to monitor the normal processing of personal data as seen in BDSG, Section 4g-1,
> Notification of the data subject according to BSDG Sections 19a and 33,
> Instructions for data subjects when data is collected according to BSDG, Section 4-3,
> Information for data subjects according to BSDG, Section 19 and 34,
> Information for the supervisory authorities in accordance with BSDG, Section 38-3.1.

The contents of the written documentation must relate to the intended purpose. For this reason it is useful to subdivide the documentation into a publicly available document (based on BDSG Section 4g-2 with 4e, No. 1–8), and a separate internal operations procedure guide that contains the information described in BDSG Section 4e No. 9 and 4g. This division fulfills various functions, but is not a legal obligation.
THE PUBLIC REGISTER
The public register is the basis for the information available to the general public, and when needed, the registration with supervisory authorities. The public register is meant to ensure general corporate transparency by providing a guide to which data is stored, and by whom, for those asking for information.

The register data should be short and understandable. The format used by the independent national center for data protection (Schleswig-Holstein) is a good example (see 2.3.9).

IN-HOUSE PROCEDURE GUIDE
The internal procedures manual, on the other hand, assists the DPO additionally with internal auditing, the process compliance test run, the identification of persons with authorized access as defined by BDSG, Section 4g-2.1, as well as with the audit of the appropriateness of measures taken as defined in BDSG, Section 9-2. It is also the basic source for information requested by data subjects. A more detailed document is required for sensitive data, such as health conditions, as described in BDSG, Section 3-9.

In many cases where a data subject must be given detailed information, relevant SAP functions (ABAP Dictionary, AIS, i.e.) can be utilized to provide supporting information.

LEVEL OF DETAIL
The information is to be provided to the DPO by the controller. Also the terms “employee groups”, “data categories” and “categories of recipients” suggest that detailed descriptions are not necessary in this documentation. Since the public register must be made available to the general public in an appropriate way, an exact description of individual data, persons, or recipients is not appropriate for the public record.

Finally, the conclusion in Section 4g-2 of the BDSG concerning security measures taken prohibits the release of the data if it presents a risk for the processing enterprise.

The documentation must, on the other hand, provide a suitable starting point for the DPO to carry out detailed analyses.

> In executing the process compliance test run the DPO may need in many cases, in addition to the table, info, and subtype descriptions, details concerning data fields (for storage of health or performance data, e.g.).
> As part of monitoring data protection compliant processing, the DPO must (in individual cases with the backing of the responsible persons and/or instructions in the documentation) be able to access data up to the field level.
> The notification covers the identity of the processor, the purpose, categories of recipients and the kind of data.
> The data subject is to be informed at the point of data collection about the identity of the controller, the purpose of the collection and the categories of recipients if they have not already been informed.
> The disclosure requires accurate information about the data stored for a person and the origin, recipients, and storage purpose of the data.
> For the evaluation of BDSG, Section 9 (measures for the guarantee of secure processing), detailed information concerning the stored data and their processing purpose is required.
From this summary it is evident that disclosures and notification also refer to topics in the system overview documentation.

The ABAP Dictionary in SAP ERP can be used for table or field analysis. The DPO must be skilled in the handling of domains, tables, reports, and application verification. In order to complete the process compliance test runs, it may be necessary to examine actual sensitive data such as fields in Infotype 0002 (personal data, religion data field), Infotype 0008 (handicap), Infotype 0028 (internal medical service) or Infotype 0077 (additional personal data, ethnic origin, religion key, veteran status). In section 2.4 it will be explained how to access contents and the documentation of fields and check tables.

It is to be noted that not all required data are electronically stored in the SAP ERP system. The general reference to the ABAP Dictionary and/or the AIS “File Register” is alone insufficient when not supplemented by written documents. As an example, there is tagging of tables and/or data fields containing personal data. In addition, purpose, recipients or persons with access rights are usually not documented in connection with the description of data or data categories in SAP ERP.

2.3.1 INFORMATION FOR THE CONTROLLER
Below points one to three of the public registration are summarized.

The information including the company name, address and the management is best suited to an Internet style Impressum.

2.3.2 PURPOSES OF THE DATA ACQUISITION, PROCESSING OR USAGE

REQUIREMENT:
BDSG, Section 4e requires a statement of the purposes of the data acquisition, processing or use.

INTERPRETATION OF THE LEGAL REQUIREMENTS REGARDING SAP ERP:
Even if the BDSG assumes the legal basis for the processing for all data is provided - i.e. for each individual data field - and must be checked prior to processing, it does not automatically follow that the written documentation is valid at the field level. The question of whether the legal basis should be included in the documentation has no concrete answer.

From the manufacturer of SAP ERP systems no generally valid statements regarding the legal requirements for user operations can be expected. This is due to the various business area laws, wage agreements, employment agreements, consent or diverse contractual relationships (BDSG, Section 28-1.1.1).

The specification of the business purposes must be defined in terms of the departments within the enterprise, e.g. financial accounting, payroll accounting, applicant data administration, travel expense accounting.
2.3.3 DESCRIPTION OF THE DATA SUBJECT GROUPS AND RELEVANT DATA OR DATA CATEGORIES

REQUIREMENT:
All data subject groups and their data or data categories are to be specified. This concerns the data protection legal definition of automated processing and not the EDP technical file term. The relationship with the terminology at the data base or operating system level should be comprehensible, but does not necessarily need to be included in the written documentation. User data must also be addressed (see below).

SAP FACTS:
SAP ERP stores its data using the services of relational database systems. Using relational links between table data at various levels can be aggregated and re-structured into new data collections.

A documentation option for data and/or tables for certain employee groups in the ABAP Dictionary is available. The following personnel groups exist:

- Employee data (HCM data)
- Applicant data (HCM data)
- Vendor data
- Customer data
- Partner data
- Specialist data
- Sales group data
- Patient data
- SAP user (master data of the user administration)

These employee groups are summarized in various report variants in the session “File register for personal data” (report RSCRDOMA). The tables used for these employee groups can be displayed in the AIS. However the AIS is still based on the phraseology of the old BDSG, using concepts like ‘File Register’ and offers so far no information about the personal data in the JAVA world. The known domains with person information are not completely shown in the AIS. In addition the SAP ERP system offers further functions for the documentation/description of data (e.g. in the ABAP Dictionary), which is presented in more detail in section 2.4.

INTERPRETATION OF THE LEGAL REQUIREMENT REGARDING SAP ERP:
Sections g and 4e-5f of the BDSG require that the controller provide the data protection officer and others a description of the employee groups concerned and the relevant data or data categories.

The question arises, exactly how specifically the employee groups and the relevant data must be documented. The BDSG leaves it to the controller, so that both the formation of data categories and the listing of individual data fields are possible.

It must be decided in individual cases for which purpose (documentation, disclosures) the information is to be used. The information must then be used only for this purpose. However No. 9 in BDSG, Section 4 requires a description which can be used to evaluate security measures. This evaluation demands, for example, an inspection of the HCM data up to the level of the individual Infotypes (and/or the DATA Dictionary table).
Personal data are stored in different circumstances in the SAP ERP system. Employee personal data is managed by personnel management (HCM). Specialist and/or user data can be used in multiple applications. Customer and vendor data is also stored.

In the SAP ERP system data about a person in relation to their various roles can emerge, e.g. in the context of payroll accounting or as accounts clerk. The distinction between different employee groups found in the Audit Information System and/or “roles” is quite suitable to fulfil the appropriate requirements of the BDSG.

The data belonging to an employee group can be queried in the AIS under the respective topic, whereby a list of non-empty tables with domain names can be displayed when desired. A list of non-empty tables is equivalent to actually used tables in a concrete system. These are the corresponding Infotypes in connection with the employee data.

The HR master data (tables PA 0*) usually differ regarding purpose, access authorization and regular recipients or can at least be divided into groups. The Infotypes in the HCM module are already predominantly structured according to personnel management or departmental (e.g. addresses, loans, social security and health insurance registration).

This supports the idea of selecting the SAP ERP system tables as the basis of the documentation. This approach has advantages, in that the determination of which tables should sensibly be summarized is avoided, and the additional data in the documentation (defined by BDSG, Section 4) can be assigned directly to the system defined tables. Also for practicability reasons this unified and system-oriented documentation is useful because the information stored in the system can be easily accessed.

In the SAP ERP implementation project it should be specified at the beginning of the customizing phase, with the participation of the data protection officer, which employee personal data can be stored. Here, in particular, the participation rights of operating and staff councils must be considered. A first draft of the data protection documentation should be developed during the customizing phase.

User data is also personal data and should be included in the documentation. For example:

- System/data entry signature, e.g. in the context of the module FI
- Log data, e.g. in the Workload analysis (STAD)
- Administrative data, e.g. authorizations for SAP users
- Data of third-parties, e.g. ordering clerk of a customer

Personal data which are exclusively used for the purposes of data protection checks, data security or data backups in legally-compliant data processing centers, are subject to a special appropriation defined in BDSG, Section 31, which should serve to reinforce the protection of data subjects.

When using system/data signatures only the fact of the processing is considered personal data, not the contents of the finished data record. If a data entry clerk enters the address of a customer and his system/data signature (e.g. personal initials), then the personal data is “employee A completed data record X on February the 3rd”.

2 Responsibilities of the Data Protection Officer
The address of the customer is not personal data of the data entry clerk. Since only the fact of the processing (and not the contents of the data records) is crucial, only the processing act itself is to be documented in the documentation. Thus it should be sufficient for SAP ERP system to list all tables, with general documentation, which contain system/data signatures.

Log files should also be included in the documentation (see also section 2.3.5). Since these records generally concern employee data, the processing of these data is subject to works council approval.

(1 sentence 6 BetrVG after § 87 exp. and/or § 75 exp. 3 sentence 17 BPersVG.)

2.3.4 RECIPIENTS OR CATEGORIES OF RECIPIENTS

It is basically the responsibility of the controller to name the recipients or categories of recipients in the SAP ERP system. Recipients may be identified from contracts with employees, as suppliers and customers (bank details) as well as from legal sources (social security, tax office, health insurance registration, etc.).

Information about theoretical recipients is found in diverse places within SAP ERP. Bank details can be found in the bank master data (table BNKA - see also SAP Audit Guidelines R/3 FI, Chapter Invoice Verification and Payment Run). Further information can be seen in the supplier master data (LFBK) or in the Human Resourced module in Infotype 0009 (Bank Details, table PA0009).

The permitted interfaces must be coordinated with the DPO during the implementation project and included in the project documentation. Whether and how data reaches these recipients is an organizational matter to be documented in a data flow plan.

Transmissions in the sense of the BDSG can be technically executed in SAP in very different ways.

In a one client installation the transfer of data can be accomplished through access rights to multiple company codes within the corporation.

A transfer of data can also occur through the transmission from one system to another system, for example, when the two systems belong to two different controllers.

Dependent on the respective technical methods there are different ways to implement the technical strategies. Some examples are given below.

WHICH HELP DOES SAP OFFER FOR THE AUDIT OF REGULAR RECIPIENTS?

> Technical connections

  Review transaction SM59 (RFC destination), Basis Services (BC-SRV) and SM54 (CPIC destination);
  additional connections: SAP NetWeaver Exchange Infrastructure, SAP XI (successor: SAP NetWeaver Process Integration, PI).
2 Responsibilities of the Data Protection Officer

WHICH OVERVIEW OF SYSTEMS AND COMPONENTS DOES SAP ERP OFFER?

> Listing of the available SAP systems with the appropriate transport layers (SE17, table TSYST or AIS?/Transport management system)
> Table logical systems (clients; Table TBDLS)
> Overview of clients - Table T000 (SC4)
> Controlling areas - Table TKA01
> Overview company code - Table T001
> Personnel area - Table TS00P
> Component hierarchy (SB01 and/or HIER)
> Workload monitor transaction ST03N (used components - monthly view in transaction ST03N; an indirect conclusion about use is possible)
> Used data tables - Transaction ST10
> Object navigator (SE84)
  Menu path:
  Tools → ABAP Workbench → Overview → Information System (SE84) → ABAP Dictionary → Database Tables and/or Program Library → Program sub-objects → Screens
> Data Browser (SE17)
  Menu path:
  Tools → ABAP Workbench → Overview → DATA browsers → Table name
> Object Navigator (SE80)
  Menu path:
  Tools → ABAP Workbench → Overview → Object Navigator

Using the Dictionary and the callable "where-used list" the use of personal data can be traced to the program level.

2.3.5 DELETION REGULATIONS

First it should be mentioned that the time-periods addressed below – concerning the destruction of personal data – are explicitly oriented to the legal regulations of the Federal Republic of Germany and to its judicial standards. Technical references and notes are, on the other hand, basically valid beyond the borders of Germany. Nevertheless, a specific implementation is required at the country and/or project-level and Customizing must take into consideration local regulations.

In accordance with BDSG, Section 3a, the collection, processing and usage of personal data and the organization and selection of data processing systems must have as a goal the least possible personal data to collect, process or use. This foundation of data reduction and data economy is one of the basic components of data protection rights. Therefore anonymization and pseudonymization should be used whenever possible.

Anonymization or "to make 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." (BDSG, Section 3 – 6)

---

10 This section is based on the following sources: Abel, data protection, volume 2, part of 6
Such an expenditure must therefore clearly relate to the purpose desired. The appropriateness of the time and effort involved must be taken into consideration.

Pseudonymization or 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.”

(BDSG, Section 3 - 6a)

Related to the information presented above, the following chapter deals with existing personal data legislation. Provisions concerning deletion deadlines and minimum retention periods are of particular importance.

Since the BDSG is however a so-called “fallback law”, special rules apply.

Only if area specific, over-riding provisions contain no legal regulations does the BDSG take effect (“Lex specialis” before “Lex generalis”).

In view of the creation of new legal regulations in the recent past, such as the general equal treatment law (AGG) from the year 2006, it can be expected that additional regulations will follow. For this reason it must be pointed out that as legislative regulations (concerning deletion and minimum retention periods) change, these changes must be put into practice.

Several legal decisions concerning deletion and minimum retention periods have already been issued. Addition decisions will surely follow. In order to maintain compliance, it will be necessary to keep on eye on data protection legal developments.

The so-called Standard periods for the erasure of data are described in BDSG, Section 4e-7. The legal definition of “erasure” in BDSG, Section 3-4 is understood as „making stored personal data unrecognizable“, where the irretrievable deletion of the data is meant, regardless of which procedure is used.11.

DATA PROCESSING BY PUBLIC BODIES

The data processing by public bodies in the German states depends on the respective state data protection laws. Where these are relevant, the BDSG does not take effect. The topic of the deletion and/or blocking of personal data by federal bodies (what is meant by this can be seen in detail in the legal definition in BDSG, Section 2-1) is discussed in BDSG, Section 20.

The following guidelines are applicable:

(2) Personal data, which are used in automated processing or are stored in non-automated files are to be deleted if…

1 their storage is illegal or

2 their content is no longer needed for the fulfilment of the tasks within the area of responsibility of the controller

(3) A data block can substitute for a data deletion when:

1 1. a deletion violates legal, statutory or contractual provisions for data preservation, or

---

11 See BDSG comment Gola/Schomerus, §§ to 3 Rn. 40
2 Responsibilities of the Data Protection Officer

there is reason to believe that the data deletion may not be in the best interests of the data subject, or
due to the type of storage media used the cost of destruction is unreasonably high.

In accordance with the principle “Lex specialis” before “Lex generalis” (that a specific law supercedes a
general law) the following examples illustrate incidences where a specific law takes precedence:

> PROFESSIONAL ASSOCIATIONS – Although there are no specific data preservation obligations for
professional associations, there are recommendations. In the Federal Law Gazette B35 for professional
associations (published October 2005) at least two years of data retention, preferably five years, are
recommended for records relating to work safety and health precautions.

> JUVENILE COURT RECORDS – Information such as decisions made by juvenile courts and court ordered
guardianship removed when the data subject reaches 24 years of age (BZRG, Section 63.1).

> TRADE BUREAU – Entries are erased after a period of three or five years depending on the size of the
fine imposed (GewO Section 153-1, 1 & 2).

> PUBLIC ARCHIVES – When documents are no longer needed by authorities in order to fulfil their tasks,
these document can be placed in the federal archives, or in certain cases in the appropriate state
archives (§ 2 exp. 1). This storage does not effect the rights of the data subjects related to the destruction
(§ 2 Abs.7) and/or legal claims concerning the destruction of personal information (§ 4 exp. 1 BArchG).

> DEBTOR DIRECTORY – Entries expire three years after the end of the year in which an affidavit was
submitted. At this point an entry can be deleted (§ 915 A ZPO, § 284 AO).

> EMPLOYMENT LAW – Data at health insurance companies, health insurance organizations and offices of
the audit committees should be deleted after four or ten years, depending on the type of data. (§ 304 SGB
V, §107 SGB XI, § 84 SGB X).

> CRIMINAL RECORDS - Entries are erased, depending on the severity of the crime, after five, ten, 15 or 20
years (§46 exp. 1 BZRG).

> TRAFFIC PENALTY REGISTER (Register of traffic offenders) – Entries are deleted after one period of two,
five or ten years, depending on the seriousness of the offence (§ 29 exp. 1 StVG).

As mentioned previously this is only an example of the existing area-specific deletion rules and the time
periods which apply to the erasure of personal data by public bodies.

However, special attention should be paid to the social insurance areas, in particular the medical insurance
deletion deadlines as described in:

> Code of Social Law (Sozial-Gesetz-Buch, I - IX). as well as
> Social Security Calculation Statute (SVRV)
> general administrative regulations for the account system in the social security system (SRVwV) and the
> Risk Structure Compensation Act (Risikostruktur-Ausgleichsverordnung (RSAV))

The data retention periods can vary between two and ten years.

The obligation for the deletion of certain data specified in (§ 284 Abs. 1 Satz 4 and § 304 Abs. 1 SGB V - data
deletion to occur as soon as these are no longer needed for the intended purposes - at the latest, however,
after ten years) overrides the deletion deadline found in § 84 SGB X.
DATA PROCESSING IN THE PRIVATE SECTOR (PRIVATE BODIES)

The specific meaning of the term “private body” is found in BDSG, Section 2-4. This definition includes all natural persons (individuals), organized persons under private law, unincorporated firms and not legally responsible associations who must adhere to the processing regulations of BDSG, Section 28.

Exceptions are the so-called loaned stock enterprises (natural or legal entities of private law, who exercise sovereign functions in their own name or on behalf of the state, such as the TÜV) as well as, according to civil law, organized organizations of federal and state public bodies in accordance with the special requirements of BDSG, Section 2-3.

Sections 35-2 of the BDSG contain a series of deletion rules. According to these rules, personal data are to be deleted if…

1. the data storage is illegal
2. the data contains information about race or ethnic origin, political opinions, religious or philosophical convictions or union membership, health or sexual preference or activities, punishable actions or infractions whose correctness cannot be proven by the controller.
3. the data has been processed and is no longer necessary for the fulfilment of the purpose of storage
4. the data is to be processed for the purpose of business transmissions and an audit at the end of the fourth calendar year since the first storage reveals that further storage is not necessary.

The “deletion deadlines” are to be differentiated from the “minimum retention period” regulations. In this regard there is a whole set of regulations which specify explicit rules based on the data content. Some of the more important areas are:

> Retention according to trade and tax law (e.g. bookkeeping, customer data, management reports, personnel data).
> Retention regulations for work, employment law, professional ethics.
> Retention regulations for data processing.

TRADE AND TAX LAW

six years (§ 257 exp. 4 HGB, §147 exp. 3 AO)
ten years (§ 257 exp. 4 HGB, §147 exp. 3 AO)

WORK AND EMPLOYMENT LAW; PROFESSIONAL ETHICS

The retention regulations extend, due to legal requirements, from:

two years Work time proofs (§16 ArbZG), protection of working youth documents (§ 50 exp. 2 JArbSchG),
five years Proofs of the Beitragsabrechung and payment of dues at social security institutions (§ 28f exp. 1 ith Vth M. § 28p exp. 1 SGB IV, paper of attorneys (§ 50 exp. 2 BRAO),
six years Operational age supply (§11 exp. 2 BetrAVG), identification obligation with financial transactions (§ 9 exp. 3 GwG),
ten years Protection of working youth documents – investigation medical examination – (§ 4 exp. 2 JArbSchUV).

Furthermore, additional special retention regulations exist for certain categories and business areas. Some examples include:
2 Responsibilities of the Data Protection Officer

> for the duration of the employer-employee relationship up to the beginning of each year.
> up to the termination of employment for an employee.
> up to the expiration of the calendar year following the last audit.
> up to the expiration of the calendar year which follows the year the lists were created.

RETENTION REGULATIONS FOR DATA PROCESSING
(BDSG, Section 9 AND Appendix for Section 9, §147 EXP. 5 AO, § 257 EXP. 3 HGB)

<table>
<thead>
<tr>
<th>Duration</th>
<th>Data Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>one year</td>
<td>Job Accounting, network data, system messages, accompanying documents and logs for data medium transport and administration, conversion logs.</td>
</tr>
<tr>
<td>three years</td>
<td>System files (three generations), standard software.</td>
</tr>
<tr>
<td>six years</td>
<td>Test schedules, shift logs, job orders.</td>
</tr>
<tr>
<td>ten years</td>
<td>User programs including all documentation about installation in the production system: system message; logs of data processing activities which must be traceable for legal reasons (accounting-relevant tables).</td>
</tr>
</tbody>
</table>

DATA PROCESSING IN SPECIAL CASES
LOG FILES
A special problem exists regarding storage of log files in automated data processing centers.

In this situation there are, on the one hand, logs related to “business” audits which concern the content changes recorded in change documents (for example, who has made posted changes, and when) and on the other hand the system log files, or Security Audit Logs (for example, logon attempts which could be blocked, cancelled processes, warning messages and miscellaneous problems. (See additional details in chapter 4.2.1.9.)

The system log files and change document logs may contain information about certain steps in the processes running in a data processing application system as well as person-recognizable data.

Individual contents of existing and/or stored log files can be assigned - without much effort – to natural persons. Because these assignments are common for the use of SAP application log files and change documents, in combination with table access, not only data protection practices but also protections provided in the Labor Management Relations Act can be affected.

Because most SAP users, and even basis administrators, are not always clear about the details concerning what, how, and where change documents are logged, or which information about software applications is logged, special attention should be paid to these activities.

The courts discovered long ago the explosiveness of log files related to data protection legislation. From the legal cases AG Darmstadt and LG Darmstadt it was learned that even dynamic IP addresses can be used to reconstruct person-related information. Because of this possibility, data protection, and where needed, employee co-determination rights must be assessed.

Thus the principles of data reduction and data economy are important for the collection and/or processing of log files (BDSG, Section 3). In individual cases it can be, however, that the employer or controller has a

---

12 See Abel, data protection, volume 2, part of 6/2.4.1.4
13 See Abel, data protection, volume 2, part of 6/2.4.1.4
14 Az.: 300 C 397/04, vom 30.06.2005
15 Az.: 25 S 118/2005, vom 25.01.2006
justified interest in the collection and storage of change document log files and system logs.

This is standardized in BDSG, Section 28-1.2:

“The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one’s own business purposes shall be admissible…. In so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use.”

In view of this specification, however, the protection-worthy interests of the data subject related to the outcome of the processing or use of the data must be kept in mind. A continuing assessment of competing interests must take place.

Unfortunately the legislators neglected, in Section 28 Paragraph 1.2 of the BDSG, to formulate concrete reference points which would simplify the assessment of interests.  

It is thus necessary that an “interests assessment” take place within a so-called proportionality audit. This audit must be carried out according to the BDSG standards as well as in the context of the legally standardized rights of codetermination of the employee representatives.

In practice that could look as follows: The more personal data included in change document log files or system logs, the higher the consideration given to the protection of the data subjects interests must be. A useful means for enabling the direct use of log files would be the implementation of tools which automatically make personal data, or data from which persons could be identified, anonymous (for example, Anonlog, Pseudo/Core). Thus with only a few payroll or tax relevant procedures would the use of classical (not anonymous) logs be necessary.

If an automated anonymization of log files is not carried out – for any reason – it is essential that the principle of limited usage (seen in BDSG, Section 31) be adhered to. This means that log files may only be used for “the purposes of data protection control or data security or to ensure the proper operation of a data processing system.”

Thus this type of data is subject to a strict “limited usage” similar to the restrictions for the public sector as described in BDSG, Section 14-4. The result is that only those persons and organizations who have a definite need for such data in order to fulfil specific tasks may access the data.

Those with access rights are most commonly work councils, data protection officials, experts and system administrators. Of course, all of these data activities should be traceable, despite the positions of trust held by these authorized users.

Here the option of “moderate” logging may be appropriate to eliminate the need for anonymization. In this case access to log files is permissible because the amount of personal data in the log files is limited. This is not the case with log files containing change documents which, due to business or tax regulation principles must be maintained. It must always be easy to discover which SAP user, for example, has cancelled an invoice. These are exactly the type of cases where logging is absolutely essential for reliable audits.
2 Responsibilities of the Data Protection Officer

JOB APPLICATION DOCUMENTS
The Federal Labor Court determined in its judgement of 6 June 1984\(^{17}\) that long-term retention of personal information forms and/or job application documents of unsuccessful applicants violated the constitutional personal rights of that applicant.

Here also the principles of data reduction and data economy apply in the sense of BDSG, Section 3. Once the hiring phase is completed, there are no good reasons which make it necessary to retain the job application information.

When the AGG took effect in 2006, paragraph 15 gave job applicants the right to legal recourse. This option allowed the applicant to sue for compensation and damages, perhaps for verbal discrimination within the process. This claim must be made within two months of the employer’s decision in order to be considered.

In this case a burden of proof exists in accordance with § 22 AGG on the part of the employer. Due to this burden of proof obligation it must be possible for the employer to keep the documents for a period of at least two months in order to meet its proof and documentation obligation.

Legal action for compensation and payment of damages must be brought in accordance with § 61b exp. 1 ArbGG ith Vth M. §15 AGG within three months after the written claim is validated.

Hence it follows that the two time periods specified above, as well as a one month waiting period, are to be added together. In summary, it can be stated that for the employer a period of six months of data retention is required.

DATA FROM DEBTOR LISTS
Trade organizations and credit bureaus, such as the SCHUFA (Credit Investigation Bureau) as a rule maintain data taken from the debtor lists (§ 915d exp. 1, § 915e exp. 1 books. b ZPO). The BDSG, Section 35-2.4 state that personal data are to be deleted, if… “they are processed in the course of business for the purpose of transfer and an examination five calendar years after their first being stored shows that further storage is not necessary.” It is necessary to check if, over and above the four year time limit, an individual case has a different time limit. The recipients of data from the debtor lists must abide by the legal deletion periods (§ 915g exp. 1 ith Vth M. § 915a exp. 1 ZPO, §15 SchuVVO - debtor listing regulation). An entry in the debtor listing is deleted at the end of three years. For debtor data, which were recorded according to (§ 26 exp. 2 InsO) should be deleted after five years.

SUMMARY
In the data protection law the data retention rules include an obligation to delete. This means the data must be irrevocably destroyed. A simple block of the access path or storage in no longer productive systems would not be permitted according to these standards. Such a delete obligation in view of the principles of data reduction and data economy is particularly important.

With relational data bases, as they are used in SAP applications, the user has, however, no influence on physical storage. Deletion means blockage of all further accesses, but not necessarily complete destruction of the data. Theoretically, they could be restored by database specialists (administrators). A data base reorganization would increase the probability that the “deleted” data are physically eliminated.

\(^{17}\) Az: 5 AZR 286/81, judgement from 6 June 1984
It is advisable to immediately delete or block, to the extent that it is technically possible, illegally stored, incorrect or suspicious data records. Data which are no longer needed for the fulfilment of the original purpose, or whose retention period has expired, should be deleted at regular intervals. Subsequently, the database – if time and technology permits it – should be reorganized. Instead of a deletion, a data block may be appropriate when the type and manner of data storage makes deletion very expensive.

The data protection officer has the responsibility to keep the controller informed of the relevant retention and deletion time frames. He should also recommend appropriate organizational measures since the implementation of the required retention and deletion regulations belongs to the DPO responsibilities (data protection is here only one aspect). Furthermore, detailed information describing the internal operations procedures for data deletion should be added to the procedures documentation.

Under certain circumstances data should not be deleted if…

> legal or contractual retention stipulations exist, or
> a reason exists to assume that the destruction of the data may not be in the best interest of the data subject.

2.3.6 PLANNED TRANSMISSION TO THIRD COUNTRIES

This point supplements the description of recipients seen in BDSG, Section 4e concerning the planned transmissions of data to third countries. In particular, countries outside of the European Union without comparable data protection standards must be examined. In this situation, the controller must pay special attention to BDSG Sections 4b and 4c. A transmission must be omitted, if the appropriate protection level is missing and thus the legal interests of the data subject concerning the protection of his data cannot be guaranteed.

Exceptions to this are, apart from consent and the transmission for the fulfilment of a contract, in particular, warranties in contract clauses or binding enterprise regulations (“Binding Corporate Rules” or “Codes of Conduct”)

The European Commission offers standard agreement clauses for special transmissions of personal data into unsafe third countries.

These standard agreement clauses are to be preferred to enterprise-created contracts. Non-standard agreements must first be approved by the regulatory authority and, after permission is granted (according to Article 26-3 in the European Union guidelines), the European Commission and other member countries must be informed.

These committees can themselves raise objections and pressure the commission to accept agreed upon, rather than exceptional, procedures.

In the USA individual companies can prove an appropriate protection level by a form of self certification (keyword Safe Harbor). The current membership list is published in the Internet. It is advisable to specify separate data categories for the respective third countries and recipients.

---

19 Link: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe harbor list
Also in the context of “Offshoring”, descriptions of the data transmitted to third countries should be incorporated into the procedures documentation. In addition, database and server support should be provided by administrators of other associated companies in third countries. Details for data processing contract work are given in chapter 5.

(21) See working document: Transmissions of personal data to third countries: Use of article 25 and 26 of the data protection guideline of the European Union (WP12)

2.3.7 MEASURES FOR THE GUARANTEE OF SECURITY
The BDSG (§ 4e number 9) demands here…
“a general description enabling preliminary assessment as to whether the measures in accordance with Section 9 to guarantee the safety of processing are adequate.”

The evaluation of the data security measures depends among other things on which individual personal data are processed. In this regard, detailed information (perhaps acquired using SAP tools – see chapter 2.4) should be included in the in-house procedures documentation.

In chapter 4 we dedicate ourselves in detail to the requirements from §9 BDSG together with data processing centers and the implementation options for SAP-ERP. In particular Authentication, user administration, authorization and authorizing will be discussed.

2.3.8 ACCESS AUTHORIZED PERSONS
Access authorizations for the data from individuals and/or person’s groups are assigned and managed through roles and/or profiles in SAP ERP. The roles and/or profiles permit and/or refuse, as a rule, the reading or changing of business or technical objects using authorization objects. The roles and profiles defined in the SAP ERP system can be assigned directly to persons or groups. Access rights can be categorized using the roles and profiles. The User Information System (transaction SUIM) can be used to display or analyze the persons with access rights in the SAP ERP system.
Example from Personnel Management (SAP HCM):

<table>
<thead>
<tr>
<th>Administrative specialist</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Compensation Management</td>
</tr>
<tr>
<td></td>
<td>Organizational Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Line Manager / Event Manager</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Compensation Management</td>
</tr>
<tr>
<td></td>
<td>Organizational Management</td>
</tr>
<tr>
<td></td>
<td>Personnel Administration</td>
</tr>
<tr>
<td></td>
<td>Personnel Cost Planning</td>
</tr>
<tr>
<td></td>
<td>Appraisal System</td>
</tr>
<tr>
<td></td>
<td>Personnel Development</td>
</tr>
<tr>
<td></td>
<td>Room Reservations</td>
</tr>
<tr>
<td></td>
<td>Training and Event Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Specialist</th>
<th>Incentive Wages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time Recording</td>
</tr>
<tr>
<td></td>
<td>Resource Planning</td>
</tr>
<tr>
<td></td>
<td>Payroll</td>
</tr>
</tbody>
</table>

For more in-depth explanations of access protection and the authorization concept refer to chapter 4.2.

References for the use of the SAP Audit Information System and the ABAP Dictionary are given in section 2.4 (System Support).

2.3.9 EXAMPLE REGISTRATION FORM

The supervisory authorities require the registration of each individual processing procedure. The suggestions of the independent national center for data protection in Schleswig-Holstein, as well as those of other supervisory authorities, are used as the basis for the following example of a registration form20.

If standard software is used in the enterprise, descriptions of certain procedures and program flows may already be easily accessed in the program documentation.

---

## 2 Responsibilities of the Data Protection Officer

<table>
<thead>
<tr>
<th>PUBLIC PART</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name/company controller</strong></td>
</tr>
<tr>
<td>Owner, executive committees, leader data processing</td>
</tr>
<tr>
<td>Address of the responsible persons place</td>
</tr>
<tr>
<td><strong>Purposes of the data acquisition, processing or use</strong></td>
</tr>
<tr>
<td>&gt; SAP ERP HCM: Personnel administration, payroll, Organizational Management, Time Management, Recruitment, Personnel Support (Compensation, Benefits, Retirement Pension), strategic personnel planning</td>
</tr>
<tr>
<td>&gt; SAP for Healthcare: Patient Management, Patient Billing, clinical order processing (partner), medical documentation</td>
</tr>
<tr>
<td>&gt; SAP EH&amp;S: Health services, industrial safety</td>
</tr>
<tr>
<td>&gt; SAP ERP FI: Care and service for customers and suppliers</td>
</tr>
<tr>
<td>&gt; SAP CRM: Marketing planning and sales campaign management, Telemarketing, contact management, customer service interaction center, Internet Customer Self service, service management, operational planning</td>
</tr>
<tr>
<td><strong>Data subject groups and relevant data categories</strong></td>
</tr>
<tr>
<td>&gt; Persons: Employee, applicant, customer, supplier, policy holder, patient</td>
</tr>
<tr>
<td>&gt; Data: Employee, applicant, customer, and suppliers’ data used in standard SAP ERP HCM, SAP ERP FI and SAP CRM; ●</td>
</tr>
<tr>
<td>&gt; Special kinds of personal data as defined in § 3 Abs.9 BDSG, e.g.: Patient data used in standard SAP for Healthcare; corporate health and/or industrial safety data used in standard SAP EH&amp;S;</td>
</tr>
<tr>
<td>&gt; Data for union membership, ethnic origin, and religion used in standard SAP ERP HCM</td>
</tr>
<tr>
<td><strong>Recipient or categories of recipients</strong></td>
</tr>
<tr>
<td>Contracting party, banks, building societies, insurance, tax office, health insurance companies, pension managers, contract data processors</td>
</tr>
<tr>
<td><strong>Data deletion time periods</strong></td>
</tr>
<tr>
<td>General: Periodic deletion at expiration of the legal retention periods</td>
</tr>
<tr>
<td>Detailed: Different retention periods for individual data types Regular determination of the need to retain a dataset</td>
</tr>
<tr>
<td><strong>Planned data transfer to third countries</strong></td>
</tr>
<tr>
<td>Data categories for third countries and recipients</td>
</tr>
</tbody>
</table>
2.4 SYSTEM SUPPORT

In the SAP system the ABAP Dictionary is designed to manage all data used in the system. The ABAP Dictionary provides information about tables, domains and fields and can be used as a “where-used” list for reports, screens or additional tables.

In this section we want to give a short review of the techniques used for producing an overview of data and data categories for the process description, as well as the audit of access authorizations. The presented functions can also contain change authorizations. These can be seen in the role definition.

System support is available to the data protection officer in the form of helpful tools such as SAP GRC Access Control (see chapter 6), SECURINFO for SAP (www.securinfo.com), ZRPDINF01 (www.forba.de) or CheckAud (www.check-aud.de), which are used especially for the analysis of authorization concepts. In this regard, the data protection officer should contact other department and/or the IT administration to verify the availability of these software tools.

Note: To assist in the understanding of the transactions used, the technical names should be included:

Menüpfad:
Extras → Settings → Display technical names
2 Responsibilities of the Data Protection Officer

2.4.1 EVALUATION OF PERSONAL DATA IN TABLES AND FIELDS

This section will describe the SAP technical means available to the controller for generating the necessary overviews needed by the data protection officer in accordance with the BDSG.

The following enumerating of tables containing personal data in standard SAP systems cannot be considered complete because customer specific additions, modifications or deletions cannot be taken into account.

With the help of the ABAP Dictionary a table overview can be produced dynamically which shows the current customer conditions.

In individual cases, “where-used” lists can be derived from domains or data elements for dependent reports, screens and tables.

GENERAL OVERVIEW

In a table overview a short description of the infotypes and/or tables can be provided. Examples:

- **PA0**  HR master data
- **HRP1**  Personnel planning data
- **PA2**  Time data
- **PB0**  Applicant master data
- **PB4**  Applicant data
- **PCL**  Cluster tables (HCM)
- **KN**  Customer master
- **LF**  Vendor master
- **SADR**  Address management

Menu path:

Menu path: Werkzeuge → Tools → ABAP Workbench → Development → Dictionary (SE12): Object name Pa 0* as database table: Display or print

With the help of these overviews targeted individual tables or fields can be accessed using the ABAP Dictionary.

We recommend that authorizations for table access to HR tables only be given to specialists with detailed HCM knowledge.

DATA IN THE PERSONNEL MANAGEMENT AREA (HCM/HR)

In the HCM the data are processed as infotypes and infosubtypes. HR master data and time data are stored in the Paxxxx tables. A PAxxxx table contains, apart from system-specific entries such as “table key”, only the data of the respective infotype xxxx.

To see details of the individual tables, use the ABAP Dictionary (SE12) or the Repository Infosystem (Object Navigator, SE84).

The following reports provide overviews of the infotypes:
> Infotypes and subtypes (report RPDSHOWI) lists the infotypes and subtypes with information about the infotype structure.
> The report RPDINFO1 provides additional database statistics concerning the infotypes and subtypes actually used in the available SAP installation.
> An overview of the infotypes in use for a specific employee is documented in the RPLINFC0 report.

These reports are also available in the Audit Information System.

In the personnel planning component personal data is linked to a person using infotype 1001 in areas such as Seminars, Qualifications, Career planning, and Preventive medical checkup.

The individual linkage (relationship) types and/or subtypes are listed in table T778V. All linkage data are stored centrally in table HRP1001. For individual linkage types (see table T77AR) additional information is stored in tables of the form HRPAD* (see table T77AD). A view of the individual tables (HRP1001, HRPAD*) can be accessed from the ABAP Dictionary as well as the RHDIC00 report.

**USER DATA 1 (USER ADMINISTRATION)**
In which tables in the SAP system, are user values stored?

Table name: US*
Domain: XUBNAME User name in the user master record

**USER DATA 2 (DATA ENTRY CLERK IDENTIFIER)**
Domains:
AENUS Username of last change
AS4USER Author of last change
BNAME User name
BUSAB Number of the accounting department clerk
DDUSER Dictionary: last user to make change
DWNAM Name of the responsible clerk
RALDB_NAME Name of the creator/changer of the variant
SACHA Clerk for payroll/personnel/time recording
UNAME User name
UBNAME User names
USERNAME User name (SAP user)
USNAM Name of the user
XUBNAME User name in the user master record
XUSER User name

**USER DATA 3 (LOG DATA)**
Log data is found in, among other places, Financial Accounting, System Log (SM 21) and in the system log files. The accounting data is identified using the payroll numbers in the user master records. The evaluation of accounting and/or the statistical records is executed using the Workload Monitor transaction.

Menu path:
Tools → Administration → Monitor → Performance → Workload → Business transaction analysis (ST03N/ST03G) → (STAD)
The user name if held in the system log file (SM21): Field name: User

2.4.2 TECHNIQUES FOR FINDING PERSONAL DATA

VARIANT 1: DURING PROJECT INTRODUCTION

In the introduction phase the permissible personal data are specified and their evaluations are examined (meaning the corresponding transactions, screens, and reports are analyzed) by the project team with the data protection officer and the operating and/or works council.

By blocking transactions and reports, as well as through screen variations created in Customizing, the input of illegal personal data can be prevented. The advantage here is that variant 2 would only be needed for additional controls.

Using the F1-Help it is possible to derive from a screen field the corresponding names of table, field, data element and domain. With this information, where-used lists for fields in programs, screens and tables can be derived from the ABAP Dictionary.

In the case where no table name, but rather a structure name is displayed, the underlying database table must be defined using the where-used function for the displayed data element.

Example: Transaction PA20 with bank details infotype:
F1-Help provides the following technical Info for bank accounts:
Screen field: P0009-BANKN
Table name: P0009
Data element: BANKN
Field name: BANKN

Menu path:
Tools → ABAP Workbench → Overview → Infosystem → ABAP Dictionary → Data elements (with selection BANKN) → Help → Where-used list → Indirect application (SE12) (here tables, program, screens, i.e. are shown)

VARIANT 2: IN THE ACTIVE SYSTEM

Tables with person-related data are not identified as personal data tables. They can, however, be located using domains with the ABAP Dictionary.

Important domains:
AFNAM: Name of the requester in the purchase order request
APLNO: Applicant number
APLNR: Applicant number
CATSXT_CALLER_ID: Identification of the initiator
DISPO: Planning manager
EKGRP: Purchasing group
KUNNR: Customer number
LIFNR: Account number of the supplier
NAME: Name of a partner
The following domains have likewise name references:

- **FALNR** Case number (in the IS-H)
- **PATNR** Patient number (in the IS-H)
- **PERSNO** Personnel number
- **PERNR** Personnel number
- **VKGRP** Sales group

The data element **GPART** Business Partner (e.g. physicians in SAP for Healthcare) may also have person-related data (domain: RI_Rolle).

In order to see a company-specific procedures tab in the Audit Information System with the help of the report RSCRDOMA, the person identifying domains specified above should be checked and supplemented if necessary (AIS function: File register to personal data).

Documentation of data fields

Functions are available in the ABAP Dictionary which allow branching to the field level of tables:

- Display and/or printing of tables and fields (also printable as table manual with RSDOCTB)
  
  **Menu path:**
  
  Tools → ABAP Workbench → Overview → Infosystem → ABAP Dictionary → Fields → Structural fields
  
  (SE84) P000* print

- Where-used list for tables, data elements and domains

  The ABAP Dictionary can be used to find information about tables, structures, field names, data elements and domains as well as their use in programs, screens and tables.
2 Responsibilities of the Data Protection Officer

Menu path:
Tools → ABAP Workbench → Development → Dictionary (with selection domains and object name “PERSNO” for personnel number) → Help → Where-used → Indirect use (SE12): refers e.g. to database tables, programs or screens.

2.4.3 AUDIT OF THE ACCESS AUTHORIZATIONS

The USER INFORMATION SYSTEM design allows it to be used to audit access authorizations.

The User Information System reports are in a tree structure and can be called using transaction SUIM. Users with certain authorizations, roles or profiles, e.g., can be identified. See also chapter sections 4.3 and/or 6.1.
Menu path:
Tools → Administration → User maintenance → Infosystem

Who is active in the system? – SM04 (user list) and/or AL08 (list of all logged-on users)

Display the active users in a defined client and/or in the entire system.

Which users (with address data) are there in the SAP system? – SUIM – Display report tree (see above)
Menu path:
Infosystem → User → Users by address data → Create list →* Display all users

CHANGE DOCUMENTS for users, profiles, authorizations and roles can be called directly from the SUIM report tree and callable in the AIS using the Change document button (reports RSUSR100, RSUSR101, RSUSR102, RSCD100_PFCG).

Use report RSUSRLOG to display the logs of the central user maintenance.

Specific selections for the analysis of a SAP Authorization Concept can also be made using the button Users by complex selection criteria for users with certain authorizations, profiles, roles and transaction codes. Selections using field values for authorization objects are also available.

> Which tables are there in the SAP system which store user values?
SE16 and SE16N DATA browsers
Table name: USR* Display of all tables with current user data
Table name: USH* Display of all tables with user change documents
See also the tables UST* and USL*.

TAANA TABLE ANALYSIS

With the transaction code TAANA:

A detailed view of the available personal data, especially for large and non-indexed data tables, can be created from the table analysis of the Archiving work field. A count of the data records for a specific field selection will be computed and saved. The selection can be temporarily (ad hoc) entered and executed.

With the transaction code TAANA _AV:
Table analysis/analysis variants can be stored and later started with TAANA.

The field selections BUKRS, VORGN, PERNR, GJAHR display, for example, for the table BSEG:

Document segment/accounting. The number of records existing for one person with the same computing code, fiscal year and business transaction key.

The field selection BUKRS, PERNR, PERNR, GJAHR, VRGNG display for the table COEP:

Controlling object line item period-based. The number of records existing for one person with the same company code, fiscal year and business transactions key.

> Which reports (ABAP) exist for User Administration?

SA 38 ABAP Reporting

Menu path:
System → Services → Reporting → Program=RSUSR* (all programs for user evaluation) → F4-Search help → Execute → Select program name → Select (= Execute)

Many important reports are available through the USER INFORMATION SYSTEM or can be started using SA38 (ABAP Reporting):

User
RSUSR002, RSUSR008, RSUSR009, RSUSR008_009_NEW

Roles
RSUSR070, RSSCD100_PFCG

Profiles
RSUSR20

Authorization objects
RSUSR030, RSUSR040

Authorizations
RSUSR030

Transactions
RSUSR010

Comparisons
RSUSR050

Where-used
RSUSR002, RSUSR020, RSUSR030, RSUSR070 (SAP-Hinweis 608661), RSUSR060OBJ

Change documents
RSUSR100, RSUSR101, RSUSR102, RSSCD100_PFCG

Additional reports:

RSUSRUSERIM User Information System

RHUSERRELATIONS User assignments display (for HCM authorization objects)

RSUSR000 Active users

RSUSR003 Check the passwords of the standard users in all clients

RSUSR005 List of the users with critical authorizations

RSUSR006 Blocked users and users with failed logons

RSUSR012 Search for authorizations, profiles and users with certain object values

RSUSR060OBJ Where-used list for authorization object in programs and transactions

RSUSR200 List of users by date of logon and change of password
3 Rights of the data subject and of the general public

RIGHTS OF THE DATA SUBJECT
The basis for the rights of the data subject is the transparency requirement of the BDSG. This means that the data subject should be told how his data will be handled at the time the data is collected (for example when signing a contract). If this does not occur, or if the data subject later requests additional information, the responsible organization is obligated to provide information to the data subject in accordance with §33 BDSG and with §6 (1), the recognition of the inalienable rights of the data subject to information (§§9, 34 BDSG), as well as the right to correct, delete or block their data (§§ 20, 35 BDSG).

In connection with the notification of the data subject, the BDSG expressly states that in the case where incorrect or incomplete information was provided, whether intentional or through negligence, a violation of the act has been committed. This can be punished with a fine up to EUR 25,000.00.

RIGHTS OF THE GENERAL PUBLIC
An additional application of the transparency requirement appears in §38 (2) BDSG. This refers to the right of the general public to see a list of all legally regulated automated data processing operations (see §4e (1), 1-8, in the BDSG).

Other details about the obligation of the controller to provide information about stored data to the general public can be found in §4g (2) of the BDSG. Here the official responsible for data protection shall provide information (described in §4e, 1-8, BDSG) in an appropriate manner to the general public upon request.

In summary, it should be emphasized that the responsibility to comply with information and transparency requirements lies with the controller, the data protection officer and local or federal officials.

However, the range and concrete implementation of the rights of the data subject and the rights of the general public are not the same. The rights of the data subject extend to every piece of personal information that has been collected about him or her.

With regard to the general public and its right to information, it is usually enough to provide the structure of the data collected, and the acknowledgement that personal data has been collected, processed and used.

3.1 Notification and Information

3.1.1 Legal Requirements
In general, personal data is stored in SAP ERP systems only for contractual reasons (work contracts, sales contracts, etc.) For this reason, the duty to inform is normally fulfilled when the data is collected (§4 BDSG) with the exception of the CRM system (see the appropriate manual). Because of this, notifications and the response to information requests (requests coming directly from the data subject) must be handled based on the circumstances.

Information provided in response to requests should be in a fixed general format, i.e. organized by data categories or by types of possible recipients. The procedures for producing the notifications (and associated documentation), as well as the design of the notifications should be established when the data processing procedures are first implemented (see also chapter 1 and 2.3).
On the other hand, the data subject has, based on the right to information, the right to request all information related to himself which is at the disposal of the controllers. The data content must be communicated to the data subject in an understandable form.

3.1.2 SAP FACTS
There is no one comprehensive report within standard SAP that gathers all personal data concerning a data subject in one step, to be displayed or printed, for the purposes of required notifications. The also applies to personal data stored in individual modules concerning a data subject whose role may be employee, customer, patient, supplier, business partner, etc., However, within individual modules there are display and printing options for specific items in the user master data records.

The Audit Information System (AIS) in SAP ERP provides assistance (see also chapter 6.1) for the use of overview functions (file register for personal data) concerning the tables or domains containing personal data.

The function “Infotype overview of an employee” is available in SAP ERP HCM (Human Resources) which can display all existing Infotype data for an employee (Personal → Personnel management → Administration → Personnel master record → Display). An information report can be produced in the next step with the transaction PA20 (Display employee master record), which can be used to print out existing Infotypes.

3.1.3 REQUIREMENTS FOR THE ORGANIZATION OF DATA PROTECTION
Since there is no standard support within the SAP system that enables users (normally controllers responsible for data protection regulations, or data protection officers and their assistants) to easily meet the requirements of the BDSG related to the obligation to provide data subject information, the user must come up with a work procedure using the means already available to meet the demands of data requestors.

A technical implementation of the organizational steps for handling information requests can contain the following elements:
> A check of the legal basis of the data request, including whether the requestor is entitled to make the request, and whether the request must legally be complied with.
> Clarification of the relationship between the data subject to the controller, which may help to narrow down the type of data needed. It can be useful to offer to assist the data requestor to identify the exact data needed for their purposes.
> Identification of the active modules which, based on the role of the data subject, could contain the data subject’s personal data.

Extraction of the data from the system: Because for this step (except for the HR functions already described) no special aids are provided, existing options must be utilized. Among these options are:

21 An update to the terminology in the current legal position of the BDSG by SAP is pending.
22 A free third-party product can be used as an alternative to Z_RPDINF001. Order from www.forba.de.
23 SAP provides, in addition, the search engine TREX/SES, which can also scan data tables and thus is suited to finding names as well as personal data. The use of the TREX/SES functions requires, however, specific search filtering rules, since search engines have no built-in data usage or confidentiality restrictions.
ABAP DICTIONARY
A procedure to extract personal data using the ABAP Dictionary and the transactions SE11 and/or SE12 follows:

1. Determination of the domains, which refer in this case to person identifying data (e.g. PERSNO (personnel number) in SAP ERP HCM, PATNR (patient number) and FALNR (case number) in SAP for Healthcare (IS-H), USNAM (name of the user with user data).
2. The tables in question are to be checked for all domains involved.
3. For each identified table, all underlying data fields should be displayed using the ABAP Dictionary or the DATA Browser (transaction SE17). If the table actually contains data about the data subject, then the data can be printed or downloaded to a text processing program.
4. In order to produce an understandable report, the key fields should be output in clear text and full field names should appear next to technical data field abbreviations.
5. Step 3 and 4 are to be repeated for all applicable tables.

MISCELLANEOUS OPTIONS
Other options for identifying applicable tables are the application hierarchy (transaction SE81) or the Repository Infosystem (transaction SE84).

USING DISPLAY TRANSACTIONS AND BUSINESS MODULE ABAP PROGRAMS
All of the display transactions and screens belonging to the respective roles must be investigated and printed documentation produced. All data not belonging to the requested information must be removed (such as the name of the person producing the report) before the final deliverable printout is produced. Relevant display transactions can be added to the user menu of the person who produces these reports (see the SAP ERP documentation concerning the set-up of “Favorites”). Relevant Reports can be made available to end-users through the Area menus (area menu maintenance with transaction SE43N).

USING REPORTS
For individual topics there are Reports or transactions which can output elements of the stored data. Examples from SAP ERP HCM:

> Personnel master data sheet (call with the report RPSTM00)
> The personnel file displays all master data for a person.
> Menu path:
  Personal → personnel management → administration → HR Master Record → Personnel file (PA10)
> Infotype overview for an employee in the Audit Information System (AIS) or directly with the underlying report RPDINF01.

Because the data structure is presented, rather than the actual stored data, each data request requires additional preparation.

USING QUERIES
If appropriate InfoSets are set up, then the requested information can also be produced with ABAP Queries. One condition, however, is that the tables and data fields in question were created with the production of relevant InfoSets.

Depending on the Query tool (SAP Query, Ad-hoc-Query and Quick Viewer) different authorizations are needed for the creation/maintenance of the Query function and for the execution of the Query function.
Dependent on the selected data source (table Join/View, functional area/SAP Query InfoSet, table, logical database) different authorizations for the execution of the Query function will be needed. For Select or the Select Option for tables or Table Joins/Views table authorizations (authorization object: S_TABU_DIS) are needed.

Queries must be classified as critical authorizations, since the table authorization groups are normally not in exact alignment with the customer system and the customer security requirements.

They should be replaced by pre-defined reports, which are converted into transactions.

Apart from that, if there is a detailed and documented authorization concept for tables, the risks at the data record/data field level can be evaluated.

SUMMARY:

> All the options presented are quite labor-intensive - except in SAP ERP HCM. For this reason, it may be advantageous to develop special Reports for frequently requested information.

> According to §34 BDSG the purpose of the storage, as well as the identification of the persons or organization receiving the data, should be part of the delivered information. These items, among other things, can be derived from the procedure listing described in § 4d BDSG and must be attached to the information. Finally, arrangements must be made to send/deliver the requested information without violating data protection regulations.

3.2 CORRECTION, DELETION AND LOCKING

3.2.1 LEGAL REQUIREMENTS

The controller must correct the data subject’s personal data, in accordance with §§20 and/or 35 BDSG, if it is incorrect. If necessary, data should be deleted (e.g. if the storage is illegal). In certain cases the locking of the personal data can substitute for a deletion. In connection with the correction, deletion and locking of data, certain questions are to be clarified beforehand:

A) CORRECTION; DELETION OR LOCK

> To which data/tables does the correction, deletion or lock requirement refer to?

> Which procedure will be used for restores and backup copies in cases of locked data?

> Do the operational system prerequisites for a deletion conform to the defined legal requirements (e.g. in SAP ERP HCM by the appropriate definition of the time constraint of the infotypes in the table T582A)?

B) HANDLING OF SPECIAL DATA TYPES

> How will log data be handled?

> Which approach is appropriate for change/deletion of access authorizations and other user master data?

> How effective are deletion and lock flags for data with double references (e.g. infotype 0021, Family Member/Dependents)?
3 Rights of the data subject and of the general public

3.2.2 SAP FACTS

There are no special SAP ERP functions - for instance transactions or report - which fulfil the requirements of §§20 and 35 of the BDSG.

However, the SAP ERP system offers, with respect to the correction of data in various application modules, the option to change incorrect data with the standard maintenance transaction, provided it can still be accessed online. Within the SAP ERP HCM, for example, the transaction PA30 (Maintenance of HR master record) can be used.

There is no built-in function which limits the access to historical records containing personal data (stored because of the data retention obligation) - even if all accounting posting procedures are finished.

The deletion of data can also be carried out with this maintenance transaction, although it should be noted that the actual deletion occurs only when the database is physically updated (the incorrect data item may still be available in the log). The incorrect data, which is still a component of the change log for infotype, can be displayed with report RPUAUD00.

There are no explicit functions in SAP ERP systems for locking the data of specific persons. Possibly incriminating data of a data subject in the SAP ERP HCM cannot be easily locked because, among other things, the corresponding authorization object P_ORGIN (master records) simply allows access to the entire infotype level, and does not check permission at the data field level.

3.2.3 ORGANIZATIONAL REQUIREMENTS RELATED TO DATA PROTECTION

In addition to the questions seen in chapter 3.2.1, basic questions concerning archiving and data deletion concepts must be addressed, and where necessary, organizational precautions implemented in reference to the following:

A) DATA LOCKING METHODS:
Because no technical function for locking individual data elements for one person is available in SAP ERP, the responsible persons or department must develop an adequate organizational procedure. As a temporary measure, the data could be archived (in compliance with data protection requirements and documentation) and temporarily deleted (in the active database).

B) DELETION PROCEDURE:
  > How does the deletion from the current dataset take place? (manually?)
  > How does the deletion from the archived dataset take place? (manually?)

C) RETENTION PERIODS (SEE ALSO SECTION 2.3.5)
  > Who is responsible for the determination of the retention periods?
  > Are the retention periods and their general conditions documented in the SAP ERP system? If so, where?
  > How does the deletion take place after the official retention period expires?
These requirements for the organization of data protection can also be integrated into the GRC Process Control (at additional cost – see Chapter 6). This allows procedures (such as the scheduled deletion of data or the reorganization of the database) to be defined and documented, and assigned to manual control. In this way routine checks can be ensured and documented.
4 Implementing the Requirements of BDSG Section 9 and its Appendix: Technical and Organizational Measures

4.1 REQUIREMENTS

This section deals with the technical and organizational requirements involved in processing and checking personal data. These requirements are general in nature and can be applied to personal data processing both within and outside of the jurisdiction of German federal law.

These regulations apply not only to production systems but also to front-end systems where personal data can be accessed or new hire information is entered and subsequently transported into the production environment.

In line with changes found in the EU Guideline 95/46/EG the required technical-organizational measures have been expanded to include protection against accidental or illegal destruction of data (Item 7: Availability Control) as well as safeguarding the limited usage of data (Item 8).

4.1.1 STATUTORY REQUIREMENTS IN ARTICLE 9 OF THE GERMAN FEDERAL DATA PROTECTION ACT

The German Federal Data Protection Act (BSDG) and, similarly, the various German State Data Protection Acts, demand that the responsible organization take technical and organizational measures to ensure that the requirements in the Data Protection Act can be met. Of particular importance are the eight detailed requirements listed in the appendix to the BSDG.

Within the scope of the SAP implementation project, coordinated, appropriate, and necessary measures must be identified and implemented at technical and organizational levels for the requirements listed in the appendix. This includes project-related risk analyses as well as the implementation of risk reduction measures at the organizational and technical levels. These measures are intended to prevent the unlawful and inappropriate processing of personal data and to enable the detection of misuse as needed.

The relevant project steps, particularly those that are related to the process compliance test run, are referenced in Section 1.

Technical solutions must be carefully coordinated with organizational procedures and responsibilities. Technical measures are ineffective if not used at the correct time and in the correct manner.

An example of an organizational mistake is the failure to take advantage of the structure of the SAP authorization concept, which, despite wide-ranging protection technical options, may offer little protection because too many users have been assigned comprehensive authorizations.

On the other hand, good organizational measures can be made ineffective. The development of a carefully worded document describing the permitted uses of personal data, as well as thorough employee training is time wasted if the download of personal data from SAP ERP is not technically prevented.
4.1.2 SAP SOLUTIONS FOR COMPLIANCE WITH THE STATUTORY REQUIREMENTS

The left-hand column in the following table shows the eight requirements found in the appendix to Article 9 of the German Federal Data Protection Act. The middle column provides recommended activities for implementing the requirements in the SAP ERP System. The right-hand column lists references to additional literature for these topics.

<table>
<thead>
<tr>
<th>REQUIREMENTS FOR DATA PROCESSING SYSTEMS (from the appendix to Article 9 of the BSDG)</th>
<th>COMPLIANCE SOLUTIONS FOR SAP ERP SYSTEMS</th>
<th>COMPLIANCE GUIDELINES AND DOCUMENTATION FOR SAP ERP SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Unauthorized persons must be denied access to data processing sites that process and use personal data (SITE ACCESS CONTROL)</td>
<td>(Concerns building security and physical access, etc. – not software.)</td>
<td></td>
</tr>
<tr>
<td>2) The use of data processing systems by unauthorized persons must be prevented (SYSTEM ACCESS CONTROL)</td>
<td>Personal logon procedure (problematic when several users are using one device); additional resources (such as chip cards and PC security systems) must ensure that users have secure logon/logoff; Automatic logoff after a specified time limit; screensaver with password protection; Single Sign-On and connection options for chip cards</td>
<td>SAP NetWeaver and SAP ERP Central Component Security Guidelines24</td>
</tr>
</tbody>
</table>

4 Implementing the Requirements of BDSG Section 9 and its Appendix: Technical and Organizational Measures

<table>
<thead>
<tr>
<th>REQUIREMENTS FOR DATA PROCESSING SYSTEMS (from the appendix to Article 9 of the BSDG)</th>
<th>COMPLIANCE SOLUTIONS FOR SAP ERP SYSTEMS</th>
<th>COMPLIANCE GUIDELINES AND DOCUMENTATION FOR SAP ERP SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>3) It must be ensured that persons authorized to use a data processing system can gain access only to the data they are authorized to access and that personal data cannot be read, copied, modified, or removed without authorization during processing or use, and after being saved (DATA ACCESS CONTROL)</td>
<td>Within SAP NetWeaver: Implementation of an appropriate authorization concept for the ABAP and JAVA stacks, which incorporates the SAP requirements, audit guidelines and data protection guidelines; External to SAP NetWeaver: Network encryption, restricted granting of authorizations for SAP files and tables at the database and systems levels; Download prevention: Improve the download function by adding an authorization check for transaction/program and enabling logging.</td>
<td>SAP Documentation SAP NetWeaver (help.sap.com) Frank Off / Mario Linkies, “SAP Security and Authorizations”, Galileo Press 2006 DSG Guidelines FI SAP NetWeaver Security Guidelines SAP GRC Access Control: Analysis and Administration of SAP Authorization Concept (Chapter 6) SAP Notes 28777, 210733</td>
</tr>
<tr>
<td>4) During electronic transfer or when saving to data storage media, it must be ensured that personal data cannot be read, copied, modified, or removed without authorization. The data transfer mechanism must provide a means for confirming the destination (receiving organization) of the personal data. (TRANSFER CONTROL)</td>
<td>Within SAP ERP: Implementation of an appropriate authorization concept for the ABAP and JAVA stacks. External to SAP ERP: Network encryption (LAN/ WAN) and other data carriers; Downloads and the XXL/ALV List Viewer (see the appendix section 8.4.3.3, Item 3) Internet: Firewall concept and SAP Router; Authorization settings; The third-party (receiving organization) verification described in BDSG, Section 10 § 4, is not supported.</td>
<td>SAP System Documentation SAP NetWeaver Security Guidelines (when needed, random sampling using Trace)</td>
</tr>
</tbody>
</table>

25 The Aquinnet.de website provides additional information including logging details and possible release of all exports (download, email, etc.) using the SAPGUI front-end.
<table>
<thead>
<tr>
<th>5) Subsequent checks must be performed to establish whether and by whom personal data has been entered, modified, or removed in data processing systems. (INPUT CONTROL)</th>
<th>Implemented systematically in all modules, for all SAP Objects, and for all data with automatic storage of creator/modifier, date, and time; in addition to display transactions, the modules provide additional reports for displaying change documents and their configuration; configuration of change documents, if needed.</th>
<th>SAP System Documentation, SAP Security Guidelines functions for the display of change documents in modules, recommendations in the SAP Security Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>6) It must be ensured that personal data processed on behalf of a customer is processed in strict accordance with the customer’s instructions. (ORDER CONTROL)</td>
<td>In general, no special measures are needed. The SAP GRC program (separate software) can be used for planning, documenting and evaluating job processing.</td>
<td>See Sections 5.2.2 and 5.2.6 of this Guide GRC Process Control (see Chapter 6)</td>
</tr>
<tr>
<td>7) It must be ensured that personal data is protected against accidental destruction or loss (AVAILABILITY CONTROL)</td>
<td>Regular data backup at database level; Data security concept; Authorizations adapted to the tasks at hand; Logging the key data modifications; Appropriate user training</td>
<td>System documentation: See the general recommendations regarding data protection in the Security Guide</td>
</tr>
<tr>
<td>8) It must be ensured that data collected for different purposes can be processed separately. (SEPARATION CONTROL)</td>
<td>Separation of systems within clients; within a client by means of the proper authorization concept (particularly for display and evaluation of the data); Within a client it is important that access to personal data external to HR/HCM and data internal to HR/HCM is separated. The combination of the two types of data could reveal employee performance and salary information. Especially sensitive are cost relevant and production related data. With evaluations of company data within a client containing personal data, it must be ensured that no cross-company evaluation is permitted or legitimized through some corresponding legal basis.</td>
<td>vgl. Prüfleitfäden des DSAG AK Revision und Dokumentation Empfehlungen der SAP-Sicherheitsleitfäden</td>
</tr>
</tbody>
</table>
4 Implementing the Requirements of BDSG Section 9 and its Appendix: Technical and Organizational Measures

The BDSG makes reference to the option of encryption procedures in the appendix to §9. SAP provides functions for the encryption of transport routes. Additional information can be found in the Security Guidelines.

4.2 SAP FACTS, RISKS, AND MEASURES

With SAP ERP, the classical ABAP world (ABAP stack) is supplemented by the JAVA world (JAVA stack). That means that in addition to the classical ABAP safety precautions, now the JAVA safety precautions must be taken. This applies in particular to BSDG Section 9 requirements, i.e. the authentication of users, user rights and logging. The following illustration clarifies this parallelism in particular for authorization checks:

```
|\---|\---|
|JAVA| ABAP|
|\---|\---|
|Web Dynpro| Web Dynpro|
|EJB| FM / BAPI|
|Open SQL| Open SQL|
```

- **Recommended**
  - Connectivity between ABAP and JAVA
  - Business relevant authority check based on ABAP roles

- **NOT Recommended**
  - Connectivity between ABAP and JAVA
  - Business relevant authority check based on UME roles
The illustration shows that accesses can be rerouted from the JAVA Presentation Layer (left) to the ABAP data through the ABAP authorization checks (right). This is typically the case with accesses to the ABAP data through a portal. The following case will clarify the legal relevance:

Links between two separate datasets (perhaps personal data from two different companies) can be made in the portal at this level using an application such as iViews. For the individual datasets this is legally permissible (for instance, through accessing a Shared Service Center).

The linkage of the personnel data of two companies, however, would be a different legal situation and no longer covered by a pure data-processing-contract relationship of two companies to a common supplier.

On the JAVA level, however, the users can manage their own datasets, although adequate authorization checks as described in BDSG, Section 9 §2-4, must also be planned for the JAVA level (this concerns the left branch of the JAVA Presentation Layer above the Businesses Layer and the Persistence Layer above the JAVA-Schema).

The following section (4.2.1) discusses the ABAP specific measures found in BDSG Section 9. A separate NetWeaver Java manual is in development for a later date and will concern itself with the JAVA specific technical-organizational measures.

4.2.1 ABAP FACTS; RISKS AND MEASURES
4.2.1.1 IDENTIFICATION AND AUTHENTICATION
4.2.1.1.1 SAP FACTS
An SAP ERP User must log on to the SAP ERP System via SAP Logon using a user ID and password before he can access the information and functions in this system. By entering this data, the user identifies himself to the SAP ERP System and the system checks whether the user is authorized to work with the system. With regard to the password, the settings made in the start parameters apply, provided no other changes have been made since the initial installation. These parameter values, which are set during installation, are provided for a test system and must be reset for the production system. Transactions RZ10 (Administration of Instance Profiles) and RZ11 (Maintain Profile Parameters) are available for managing the parameters.

The parameters relevant for identifying the user are explained in the following table. The Options and Recommendations specify a basic level of protection and are based on practical experience. It should be noted that the parameter values can be defined quite differently in each company, depending on the company’s security policy.
<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
<th>OPTIONS AND RECOMMENDATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length of password</td>
<td>The LOGIN/MIN_PASSWORD_LNG parameter determines the minimum number of characters the password must contain.</td>
<td>Starting with SAP NetWeaver 6.40 the system default is 8.</td>
</tr>
<tr>
<td>Composition of password</td>
<td>The parameters login/min_password_letters, login/min_password_digits, und login/min_password_specials allow the specification (up to and including SAP NetWeaver 6.40) of minimum values for alpha-characters, digits, and special characters in a password (not case-sensitive).</td>
<td>The recommended value for each of the three parameters is 1. (The minimum number of characters, digits, and special characters equals one character space.) Caution! – Because of the various keyboard layouts in international installations, the limitations on special characters should be waived.</td>
</tr>
<tr>
<td>Minimum number of lower and/or uppercase letters in a password</td>
<td>Starting with SAP NetWeaver 6.4 the minimum number of lowercase and uppercase characters required in a password can be set using the min_password_lowercase and login / min_password_uppercase parameters.</td>
<td>The recommended value for both the login/min_password_lowercase and login/min_password_uppercase parameters is „1”.</td>
</tr>
<tr>
<td>Minimum wait period until next password change</td>
<td>Up to and including SAP NetWeaver 6.40 a user could change their password once per day, every day. Since then, the parameter login / password_change_waittime can be used to increase the required time between password changes.</td>
<td>Recommended value for the login/ password_change_waittime parameter is “1”.</td>
</tr>
<tr>
<td>Password history</td>
<td>Up to SAP NetWeaver 6.40 the SAP system checked if a new password was identical with the user’s 5 most recently used passwords. If identical, the new password was rejected. Starting with SAP NetWeaver 6.40, the parameter login / password_history_size allows the system to check up to 100 old user passwords when a password change is attempted.</td>
<td>Recommended value for login/ password_history_size: „12”</td>
</tr>
<tr>
<td>Minimum difference from previous password</td>
<td>Starting with Web AS 6.10 the security administrator has been able to set the number of characters which must be different from the old password in the parameter login / min_password_diff.</td>
<td>Recommended parameter value for login/ min_password_diff: is „4“</td>
</tr>
<tr>
<td>Compliance with current password policy</td>
<td>Starting with SAP NetWeaver 6.40 the parameter login / password_compliance_to_current_policy can be used to check passwords already in use to determine if they are in compliance with current password policy. When not, a password change is forced.</td>
<td>Recommended setting: 1 (activated)</td>
</tr>
<tr>
<td>Expiration period for the password</td>
<td>The LOGIN/PASSWORD_EXPIRATION_TIME parameter determines the interval for changing the password for dialog logon and ITS services that use the flow logic.</td>
<td>Recommended parameter value: “60” or less (the user must change his password before a maximum of 60 days.)</td>
</tr>
<tr>
<td>Maximum idle days before blocking of user-defined password</td>
<td>Starting with SAP NetWeaver 6.40 the parameter login / password_max_idle_productive can be used to specify number of days a password is unused before it is blocked.</td>
<td>Recommended parameter value for login / password_max_idle_productive: „30“</td>
</tr>
<tr>
<td>Maximum idle days before blocking of unchanged initial password</td>
<td>Starting with SAP NetWeaver 6.40 the parameter login / password_max_idle_initial can be used to specify how many days an initial password can be unused before it is blocked.</td>
<td>Recommended parameter value for login / password_max_idle_initial: „3“</td>
</tr>
<tr>
<td>Illegal passwords</td>
<td>Apart from the settings already mentioned, passwords excluded from use (for example, trivial passwords or keyboard combinations) can be defined in the table USR40.</td>
<td>The number of entries normally falls between 15 and 40.</td>
</tr>
</tbody>
</table>
### Additional Logon Variants

Depending on the Release, there are additional logon variants in addition to the password-based logon, such as:

- Certification logons via the browser and Web server
- SAP logon ticket (for example, using a SAP NetWeaver Portal)
- NT domain logon (NTLM)
- PAS (Pluggable Authentication Services), Single Sign-on

### Ending the SAP Session

The LOGIN/FAILS_TO_SESSION_END parameter determines how many failed logon attempts are permitted before the SAP session is ended. If the session ends automatically, this is registered as a failed logon attempt.

**Recommended parameter value:** "3" (The session is ended after 3 failed attempts.)

### Possible Logon Attempts

The LOGIN/FAILS_TO_USER_LOCK parameter controls how many logon attempts are permitted before the user is locked.

**Recommended parameter value:** "5" (The user is locked after 5 logon attempts.)

### Unlocking at Midnight

If the LOGIN/FAILED_USER_AUTO_UNLOCK parameter value is set to "1", users who have been locked due to incorrect logons are unlocked at midnight.

**Recommended parameter value:** "0" (automatic unlocking does not take place at midnight.)

### Automatic Logoff when Inactive

The RDISP/GUI_AUTO_LOGOUT parameter controls how much time in seconds is permitted before the user is automatically logged off. When a user is automatically logged off, data that has not be saved is lost, which results in the risk of data loss in the event of a “forced” logoff.

**Recommended parameter value:** "0" (The SAP ERP System does not automatically logoff. Instead of the SAP automatic logoff with the risk of losing data, a password-protected screensaver should be activated after 15 minutes.)

---

In the same way that the procedure for logging on to the system is controlled by parameters, the authorization checks in the SAP ERP System are based on profile parameter settings. The recommended settings listed in the following table again afford a basic level of protection. The following key parameters are of special importance:
Deactivating Authorization Checks  
Authorization checks can be suppressed with the AUTH/NO_CHECK_IN_SOME_CASES parameter. The number of authorization checks proposed by SAP can be reduced by using transaction SU24. This presupposes that the parameter is set to “Y” for deactivating the authorization checks. The value must be set to “Y” if the profile generator is used.

Starting with SAP NetWeaver 6.40 the system default is 8.

Authorization Checks for RFC  
The parameter AUTH/RFC_AUTHORITY_CHECK determines whether authorization checks are carried out for the authorization object S_RFC for Remote Function Calls (RFC).

Recommended parameter value: “1” (the authorization check for RFC is active.)

Authorization Check for ABAP Statements  
The AUTH/SYSTEM_ACCESS_CHECK_OFF parameter enables automatic authorization checks to be deactivated for specific ABAP statements. These statements are, for example, file operations, kernel functions calls, or CPIC calls.

Recommended parameter value: “0” (The authorization check for ABAP statements is active.)

4.2.1.1.2 RISKS AND MEASURES TO BE TAKEN
The following measures are suitable for minimizing the risk of impermissible access to the SAP ERP System and for activating the basic security mechanisms of the authorization concept instruments provided in the SAP ERP System:

> Defining the target values for the profile parameters and “illegal” passwords on the basis of a company-specific security concept.
> Adjusting the values of the profile parameters (transactions RZ10, RZ11)
> Maintaining the “illegal” passwords table (table USR40)
> Regularly monitoring the parameter settings (RSPARAM report or with the Audit Information System: transaction TU02 for the display of changes)
> Regularly monitoring the “illegal passwords” table using transaction SE17 (Data Browser) for table USR40 or with help from the Audit Information System

In addition or alternatively, depending on the overall IT architecture in which an SAP ERP System is included, further external security products are recommended. Such products include SNC (Secure Network Communications) or X.509 Client Certificates when using Web front-ends. For SNC, the cryptographic library...
is available for downloading from the security homepage (http://www.service.sap.com/swdc -> Download -> SAP Cryptographic Software)). See also SAP Note 397175.

4.2.1.2 STANDARD USERS
There are a total of four standard users in the SAP ERP System. The function of these users is described in the following sections. It is particularly important that these standard users be protected within the scope of the technical and organizational measures.

4.2.1.2.1 SAP*
The SAP* user is the start-up user provided with fixed-rights by SAP and, therefore, has all authorizations for the installation phase. Following the initial logon (for initial password, see the SAP NetWeaver Security Guide) in the SAP System, a new user (unique assignment by name) must be created with comprehensive authorizations. This user is responsible for further administrative tasks.

Even if the SAP* user is not needed to carry out other activities, SAP* must not be deleted, as otherwise, provided no other technical measures are taken, all other users will be able to log on as SAP* using the standard password. Each time SAP* logs on, the user obtains the specific system rights associated with this user master record.

Consequently, for security reasons, SAP recommends that you withdraw all authorizations, or that the authorizations be restricted to display functions. SAP* should also be assigned to the „SUPER“ user group to prevent this user from being deleted inadvertently; that is, SAP* cannot be physically deleted. If someone deletes SAP* via SU01, for example, SAP* will no longer be displayed in the user list, but will continue to exist in the system.

If the above measures are not taken, a new logon can be prevented via the following parameters:

Login/no_automatic_user_sapstar with value “1” (Automatic SAP* user is deactivated)

Starting with NetWeaver 7.0 the default value of the profile parameter was changed to 1, thus the SAP* user is automatically deactivated.

4.2.1.2.2 SAPCPC
The SAPCPC user is a specially defined standard SAP user. It cannot be used to log on for dialog processing, but allows some programs and function modules to be called in the SAP ERP System. This user is needed for collecting performance data, starting external background programs, and returning values for the Computer Center Management System (CCMS).

As a protective measure, the user can be locked in addition to changing the standard password. SAP Note 29276 should be consulted when implementing these measures.

In general, CPCI users should have function-related roles/profiles, even though they cannot log on for dialog processing.
4.2.1.2.3 DDIC

In addition to SAP*, the DDIC user is uniquely defined by SAP. The DDIC user is used to maintain the ABAP Dictionary and software logistics. As a result, extensive system rights are also stored for this user, in addition to those defined in the user profiles.

When the system is installed, DDIC is created only in clients 000 and 001 (for the initial password, see the SAP NetWeaver Security Guide). If necessary, the DDIC user must be created for other clients.

Since DDIC is a user with special rights and is generally difficult to assign to one person, the use of DDIC is also subject to special requirements with regard to the traceability of the activities carried out.

From the point of view of data protection, the SAP_ALL profile is not allowed for the DDIC user. Function-related profiles/roles should be created in order to perform the necessary activities (such as starting and stopping system monitoring tasks). Moreover, organizational stipulations must be made to identify which employee is using DDIC (clear responsibility).

In order to protect the DDIC user, the standard DDIC password must be changed, and when not in use, it must be blocked. Of course, neither the user nor his profile may be deleted. The DDIC user is needed for tasks during installation, upgrading, software logistics, and the ABAP Dictionary. If the DDIC is deleted, functionality will be limited in these areas.

4.2.1.2.4 EARLYWATCH

The EARLYWATCH user is the dialog user for the EarlyWatch Service in client 066. SAP EarlyWatch experts work with this user and it is needed for the EarlyWatch Monitoring and Performance functions.

In order to protect this user from unauthorized access, the initial password must be changed. Technical and organizational measures must also be taken here to ensure that only those functions are carried out that are intended for this user.

4.2.1.2.5 BATCH USER

The Batch user is provided to serve primarily as a technical user. It should be assigned to all relevant procedures. In addition, for each procedure only the necessary authorizations should be assigned.

4.2.1.2.6 RISKS AND MEASURES TO BE TAKEN

Special technical and organizational measures must be taken in order to combat the risk of unauthorized access to the SAP ERP System. When taken, these measures ensure that unauthorized viewing and unintentional/intentional manipulation of data is prevented. This applies specifically to special users.

The following measures should be taken:
> Create function-related roles/profiles for the above-mentioned users
> Lock users who are not required for day-to-day activities, or who are not active
> Configure the system parameters (see, for example, preventing logon with the SAP* user) in order to prevent unauthorized logons
Regularly monitor the activities of the above-mentioned users
Establish/create procedures for handling special users to support the technical measures

4.2.1.3 USER AUTHORIZATION CONCEPT: SELECTED AUTHORIZATION OBJECTS
Key authorization objects from the HCM module and Basis will be discussed in the following section. Complete documentation for authorization objects can be obtained in the profile generator (PFCG) by double-clicking the authorization object. In older systems, this documentation is only available for the individual authorization objects in transaction SU03 or via the Audit Information System (transaction SUIM).

4.2.1.3.1 AUTHORIZATION OBJECTS IN THE HCM
The authorization object P_ORGIN (HR: master data) is used as part of the authorization check for employee data (master record and time data). A check is generally performed when HR Infotypes need to be processed. The essential components are the organizational assignment of the HR master data, the data view (InfoTypes), and the authorization level.

The authorization object consists of the following fields:
- **AUTHC**: Authorization level
- **INFTY**: InfoType
- **SUBTY**: Subtype
- **PERSA**: Personnel area
- **PERSG**: Employee group
- **PERSK**: Employee subgroup
- **VDSK1**: Organizational key

The following values are also important with regard to the authorization level (see the SAP Object documentation for further details):
- **R**: Read
- **W**: Write
- **M**: Read with input assistance. (Matchcode) (Recommendation: Never assign just W or just R. This prevents the users from obtaining search help (previous matchcode search) and forces them to directly enter personnel numbers.)
- **S**: Unlock a write lock, provided the last person to change the record was not the current user.
- **E**: Writing locked
- **D**: Change the lock indicator
- *****: All operations

Besides the authorization object P.ORGIN, there are 4 authorization objects which are additionally or alternatively checked as needed when user master data is accessed by department employees. These are:
- **P.ORGINCON**: HR: Master record with context
- **P.ORGXX**: HR: Master record extended check
- **P.ORGXXCON**: HR: Master record extended check with context
- **P.PERNR**: HR: Master record personnel number check
The authorization objects P_ORGINCON and P_ORGXXCON enable the additional check of a structural authorization profile from the table T77UA. On the other hand, the authorization object P_PERNR is used to restrict access to a personnel number (in case of the ESS scenario) or to prevent the maintenance of a personnel number (other than by the employee assigned to the number).

In addition to the authorization objects described above for HCM master data, an authorization for each respective transaction is needed for master data maintenance, e.g. PA30 (user master data maintenance).

It should also be taken into consideration that, when necessary, additional authorization objects (e.g. HR: Applicant or Fi: Travel_Planing) may be needed for checking purposes (for further details see the SAP Authorization Object documentation).

4.2.1.3.2 AUTHORIZATION OBJECT P_ABAP

Two authorization objects are provided in SAP for protecting access to reports. The first of these is S_PROGRAM (ABAP: Program Flow Check, object class BC_C) and the second is the HR: Reporting object P_ABAP.

The object S_PROGRAM is used first to specify which reports can be accessed with the transactions SA38, SE38 and START REPORT, provided the user is authorized to access the authorization group of the report (see Section 4.2.1.5.4 below).

The P_ABAP object controls how the objects:

> HR: Master Data (P_ORGIN)
> HR: Master Data – extended check – (P_ORGXX)
> Structural authorization check in specific reports

…available for checking HCM InfoType authorizations, are used or restricted.

By appropriately configuring the fields:

> REPID (Report name), and
> COARS (Degree of simplification for authorization check),

the check of InfoType rights can be overridden, that is, they can be removed from the check.

SAP created this authorization object to enhance processing by “deactivating” additional authorization checks.

As a result, the attributes of this object must be examined critically to ensure that personal data cannot be displayed with the reporting function.

4.2.1.3.3 AUTHORIZATION OBJECT P_TCODE

The object P_TCODE is an application-specific authorization object and was a precursor to the authorization object S_TCODE. The attributes of the authorization object P_TCODE (HR: Transaction Code) enable the access to various HCM transactions to be protected.

Note that this object is not used for all HCM transactions, which means that the object S_TCODE must also be used. The tables USOBT and USOBX can be used to determine which transactions are protected by the attributes of the object P_TCODE. These tables are evaluated for the object by entering “P_TCODE” in transaction SE17.
4.2.1.3.4 AUTHORIZATION OBJECT S_TCODE
When transactions are called, the authorization object S_TCODE checks whether the user is authorized to execute the selected function. The Transaction code (TCD) field is defined for this object.

Configuring this object for specific functions enables access protection measures to be mapped during the first step in the process. Provided that no further settings are defined for this object, the module or function-specific objects are used in the remaining authorization checks.

All of the objects that correspond with one another must be configured accordingly to ensure that the requirements of the German Federal Data Protection Act are sufficiently covered.

Using the transactions SE38, SA38 and START_REPORT it is possible to execute most of the available standard reports without a check of the corresponding authorization occurring.

This can be prevented using the protective measures described in section 4.2.1.5.4. The transaction sub% should not be assigned to a user. A user can start any transaction with this right, and no authorization check will be carried out (see SAP Note 842915) With sub% Reports can also be executed, but in this case the rights will be checked.

4.2.1.3.5 TABLE TSTCA
All the transactions with additional check objects are stored in table TSTCA. The table can be evaluated using transaction SE17.

This table is subject to the workings of the CTS and CTO (Change Transport System and Change Transport Organizer), since cross-client entries are maintained in it.

The “transaction start check” is stored in the table. A context-free check occurs to determine whether the object with the specific values is present in the user buffer. An investigative check (of activities related to an object characteristic) takes place in the program run. The check of objects can be disabled in the USOBT table. This does not apply, however, to HCM and basis objects.

Note that access authorization checks can be bypassed by deactivating the Authority Check in the ABAP program containing the transaction code.

4.2.1.3.6 CONVERTING REPORTS TO TRANSACTIONS
SAP provides two options for assigning reports to transactions. The first is automatically carried out when the report is integrated into an area menu or role menu. There is, however, no obvious connection between the report and the transaction name, as SAP numbers the transactions consecutively (structure S_XXX_xxxxxxxx). For this reason, the second method is preferable: Reports are stored with a transaction set by the user and are started by calling this transaction. With both methods, note that the user can also start the reports via the “normal” reporting function if he has authorization to use transactions such as SA38 or SE38. Reports can also be started indirectly from SE80 and SE84, as well as with various other transactions.
From the point of view of the Data Protection Act:

a. A concept for protecting the individual reports must be developed (authorization concept S_PRO
GRAM, administration report RSCSAUTH), and

b. An analysis must be performed to determine whether, and to what extent, the authorization checks
can be circumvented, using the methods described above.

Authorizations for the transactions SA38 (ABAP program execution), SE38 (ABAP editor) and START_RE:
PORT should not be assigned to the users in departments. Instead, it is advisable to generate transaction
codes for the approved reports. Access to these transaction codes can be made available to the individual
users through the user menus (authorization object S_TCODE).

4.2.1.3.7 AUTHORIZATION OBJECTS S_TABU_DIS, S_TABU_CLI AND S_TABU_LIN

The object S_TABU_DIS controls access to table maintenance functions using transactions such as SE16,
SE16N, SE17, and SM30 – SM34. The authorization object S_TABU_CLI controls the access to the cross-client
table maintenance functions. In addition to the appropriate settings for these objects, transaction authoriza-
tions are required for maintaining tables (see S_TCODE).

The authorization object S_TABU_DIS consists of the Activity and Authorization Group fields. The type of
access to tables (display or change) can be controlled by setting the Activity field accordingly. The Authoriza-
tion group field is used to restrict access to certain tables.

The authorization object S_TABU_CLI consists of the field “Cross-client maintenance indicator”.

The authorization object S_TABU_LIN defines authorizations for the display or maintenance of table
contents. The object supplements the authorization objects S_TABU_DIS and S_TABU_CLI.

While S_TABU_DIS works on the level of customizing tables or maintenance views, S_TABU_LIN can be
used to control access to individual table rows.

One condition for the use of the authorization object is the existence of business organizational criteria.
Organizational criteria define business organizational units (e.g. a country or a plant) and represent a
relationship between key fields in tables and the authorization fields of S_TABU_LIN. They are defined in
Customizing (IMG Path SAP NetWeaver → System Administration → Users and Authorizations →
Line-oriented Authorizations → Define Organizational Criteria).

An authorization at the row level works only if the associated organization criterion in the appropriate client
is enabled (SAP NetWeaver → Application Server → Basis Services → System Administration → Users and
Authorizations → Line Related Authorizations → Activate Organization Criteria).

It is recommended that the transactions SE16/SE16N/SE17 be very restrictively assigned to users.

From the point of view of the Data Protection Act, access to the authorization groups for these tables (for
example, the InfoTypes in the PA table) should be restricted to prevent unauthorized access to personal data
with transaction SE16/SE17.

Tables can be assigned to authorization groups by calling transaction SE17 and specifying the table TDDAT,
or by calling transaction SE53 (Generate table maintenance dialog).
4.2.1.3.8 AUTHORIZATION OBJECT S_TOOLS_EX

Authorizations can be assigned via the object S_TOOLS_EX (object class BC_A). These authorizations are used to display externally captured statistics when monitoring tools are running.

This object contains a field (AUTH) which can be used to assign authorization names. The entry S_TOOLS_EX_A allows access to external statistics.

To prevent service and behavior checks from being performed, this access should be restrictively assigned. User behavior may only be evaluated in reasonable and agreed upon special cases.

Particular attention must be paid to the co-determination rights of the employee representation board when this authorization is assigned.

4.2.1.3.9 AUTHORIZATION OBJECT S_SCD0

The authorization object S_SCD0 (change documents, object class BC_Z) provides access to change documents and change document objects. Change documents are created when records such as master data and user master records are modified.

Change documents (master data) form part of documents (long-term documents) that must be kept pursuant to Article 257 of the German Commercial Code. Change documents and change objects can be modified or deleted in SAP by appropriately configuring the authorization object S_SCD0 (see User authorization concept), and, therefore, can directly influence the logging function.

Particular attention must be paid to the co-determination rights of the employee representation board when this authorization is assigned.

4.2.1.3.10 OBJECTS FOR USER AND AUTHORIZATION MAINTENANCE (S_USER_XXX)

The authorization objects for user and authorization maintenance (see details in section 4.2.1.6.1) enable the processes for creating and maintaining users and assigning users’ authorizations to be tailored to the company’s needs.

As far as data protection legislation is concerned, these processes must be carefully configured so that access is reserved for authorized persons only.

4.2.1.3.11 AUTHORIZATION OBJECT S_GUI AND XXL LIST VIEWER

SAP offers the option to transfer a wide variety of evaluations from the “secure SAP Environment” to a PC either by downloading or by using the XXL List Viewer. This data can then be processed without any additional checks. In general, all data that can be displayed on the screen due to authorizations assigned to the user can also be transferred to the PC. The XXL List Viewer functions can currently be protected to a limited extent by the authorization object S_OLE_CALL.

SAP provides the authorization object S_GUI to protect the download function. Only the “Activity” field is currently defined for this object. The value “61” authorizes the user to save all the results that can be
displayed on the screen as local files. Additional authorization checks (for started reports and transactions, for example) can be added via a user exit (see SAP Note 28777, 210733 und 510399).

4.2.1.3.12 AUTHORIZATION OBJECT S_SPO_DEV
Authorizations can be assigned for printing on printers named via the authorization object S_SPO_DEV. By generically assigning printer names, for example, you can specify that users of the HR module can only print on printers in the HCM department.

4.2.1.3.13 RISKS AND MEASURES TO BE TAKEN
To prevent the risk of unauthorized access to personal datasets, the above objects must be configured in such a way that only the data relevant for the tasks in the work center in question can be read and managed.

For operations in Human Capital Management, an appropriate configuration of the user authorization concept should ensure that access to the objects named above and to all other objects in the Human Resource class is restricted and complies with the “segregation of duties” model. Access to all InfoTypes should be strictly limited.

In particular it must be ensured that:
> Technical and organizational measures are put in place to deny the access required for changing and deleting change documents. Any access via reports, such as RSCDOK99, must be prevented.
> Data can only be downloaded as authorized, that is, it must be ensured that the authorization concept is adequately configured so that only function-based data access is possible
> Misuse of the data by the download function and/or the XXL/ALV List Viewer is prohibited and that subsequent processing for purposes not permitted by the Data Protection Act or for impermissible reasons (such as inadequate auditability) is excluded
> Table display and maintenance authorizations are adequately restricted by the configuration of the authorization class field
> Access, in terms of the options for changing transactions and programs, is handled in an extremely restrictive manner, or that access is prevented by means of organizational rules (including the creation of organizational instructions regarding the procedure documentation for the maintenance measures to be taken)
> As a rule, change documents cannot be deleted in the production system (with the exception of emergency users), or by the archiving and reorganization programs provided
> The authorization level field is defined restrictively with regard to access to HCM InfoTypes
> The authorization objects P_TCODE and S_TCODE are appropriately configured

In situations where a smaller workforce makes it impossible to strictly comply with the “segregation of duties” model through the configuration of the authorization objects named above, it is recommended that the organizational instructions stipulate the use of downstream checks. A neutral department should check compliance at regular intervals.
4.2.1.4 USER AUTHORIZATION CONCEPT: SELECTED PROFILES

System administrators must be set up in order to be able to carry out the necessary system administration tasks. These system administrators naturally have extensive authorizations. For this reason, SAP generally provides the following delivery profiles in the standard system for use in the test system. These delivery profiles must, however, be adapted to satisfy the requirements of the company.

In the event of an emergency, or in the event of an upgrade or release upgrade, comprehensive rights (authorizations or profiles) may have to be assigned temporarily. Note that a different person assigns these authorizations (double-verification principle) and that it is ensured that these users and authorizations are deactivated after the required usage time.

Emergency accesses by critical users represent a significant problem for the administration. The monitoring should include, in addition to the double-verification principle and the activation of the Security Audit Logs, a relevant approval procedure and a detailed follow-up evaluation. The GRC Access Control (to be purchased separately – see chapter 6) program provides a Super User Management solution.

4.2.1.4.1 SAP_ALL PROFILE

This profile grants nearly unrestricted access to the entire system (including applications). This includes access to application development tools, as well. The use of the various authorizations contained in this profile can thus endanger data storage and data processing, as described in the German Federal Data Protection Act, as well as legal compliance in financial accounting.

The profile can be re-generated by the customer as needed.

4.2.1.4.2 SAP_NEW PROFILE

The SAP_NEW profile provides authorizations for new authorization objects for existing functions. The individual fields of the objects contained in the SAP_NEW profile are generally set to comprehensive values (*). SAP_NEW is shipped on a release-specific basis.

Since the object configurations contained in SAP_NEW, in connection with the authorization concept implemented in the company, leads to unwanted authorization enhancements, this profile should not be assigned to any user in SAP production systems.

4.2.1.4.3 P_BAS_ALL PROFILE

SAP also ships standard profiles for the HCM area in test systems. The P_BAS_ALL profile (all authorizations for personnel data) enables comprehensive access to personal data. Furthermore, the contents of other applications can be displayed by the general table display functions. This profile should not be used in production systems.

4.2.1.4.4 OTHER S_XXX PROFILES

The profiles described in the following are simply models. In general, the settings for the individual authorization objects in these profiles must be restricted based on their function.
4.2.1.4.5 ROLES WITH CRITICAL AUTHORIZATIONS

Roles can be analyzed using various criteria in the User Information System (transaction SUIM\textsuperscript{26}). Some options are:

- Role based on an authorization object (e.g., P\_ORGIN, HR: Master data). The role is displayed with authorizations for the HR master data (using the authorization object P\_ORGIN). Searches for roles with (critical) transactions, authorizations or profiles can also be executed.

- User with critical authorizations (e.g. Variant SAP\_RSUSR009). After the role name is entered the critical authorization is displayed along with the users assigned to the role and other information (report RSUSR008\_009\_NEW).

Note: The SAP suggestions concerning critical authorizations focus primarily on the technical side. To make optimal use of these reports, the critical authorizations must be configured by the user.

With SAP GRC Access control (to be purchased separately) it is possible to analyze the roles and authorizations assigned in the SAP system. Critical authorizations are identified on the basis of pre-defined rules (see also chapter 6).

4.2.1.4.6 RISKS AND MEASURES TO BE TAKEN

Um dem Risiko der unzulässigen Zugriffe auf das SAP ERP-System zu begegnen und die grundsätzlichen Schutzmechanismen der im SAP ERP-System zur Verfügung gestellten Instrumente zum Berechtigungskonzept zu aktivieren, sollten die o. g. Profile grundsätzlich in einem Produktivsystem nicht vergeben werden. Dies ist v. a. aufgrund folgender Sachverhalte erforderlich:

- Checking or traceability is not provided by the use of the replace function when debugging or deleting change documents (part of the authorizations in SAP\_ALL)

- The data protection requirements are violated due to a failure to adapt the authorization concept,

- Access protection for the SAP ERP System is circumvented by use of developer rights (in particular, circumvention of the authority check),

- By-passing of the access rights needed for the logical databases by direct reading of the transparent tables (e.g. by access to the tables of the HR master data (PAxxxx)). Scan the Report sources with RSRS\_SCAN\_ABAP\_SOURCE to identify direct accesses to critical tables without authorization check.

- By-passing the separation of clients through the use of the ABAP SELECT command with the CLIENT-SPECIFIED option - check as above.
The system status is changed, for example, when:
> Access authorizations are assigned to an unauthorized user or for impermissible programs
> Files, data fields, or keys that have not been approved are configured
> Infringements are concealed by changing the system parameters, for example by:
> Falsifying the log files, for example by temporarily deactivating table logging. This, however, requires
access to the profile parameters, the table activation authorization, or the developer authorization
> Circumventing access authorization checks by deactivating the authorization check

The “standard profiles” shipped by SAP must generally be adapted in terms of their functions to satisfy the company’s requirements and ensure adequate access protection that complies with the various statutory requirements.

The exception to this requirement is the option to assign an extensive profile to emergency users. An example of this is the profile SAP_ALL delivered by SAP, whose authorizations should be reduced to the deletion or deactivating of logging (object S_SCD0).

**4.2.1.5 SPECIAL FEATURES OF THE AUTHORIZATION CHECK**

**4.2.1.5.1 DEACTIVATING AND MODIFYING AUTHORIZATION CHECKS**

As presented in section 4.2.1.1 (Identification and Authentication), authorization checks can be deactivated with the appropriate parameter settings.

It is also possible to globally deactivate the check of individual authorization objects in SAP ERP systems using transaction SU24, SU25, or SU26. Exceptions to this are the Basis and HCM module authorization objects. Those beginning with S_xxx and P_xxx can not be globally disabled in this way. The authorization checks of the Java stacks (UME27 roles) will not be globally deactivated using these transactions.

The transactions SU25 and SU28 include various activities such as “Installation of the Profile Generator” or “Transport of Customer Tables”. The global disabling of authorization objects using SU25/SU28 is carried out with help from transaction AUTH_SWITCH_OBJECTS.

From the data protection viewpoint the deactivation of authorization objects is problematic. The following protective measure can be taken:
> Blocking of the AUTH_SWITCH_OBJECTS transaction using transaction SM01 (Block/Unblock transaction codes).
> Setting the profile parameter auth/object_disabling_active to the value “N” (in order to suppress the authorization checks for specific authorization objects, the profile parameter auth/object_disabling_active must be set to the value “Y”).

For those exceptional cases where the global deactivation of individual authorization objects is permitted, at a minimum the following recommendation from the SAP documentation should be implemented:

For the securing/activation of deactivated authorization checks for authorization objects an authorization for the S_USER_OBJ object will be needed. For security reasons the authorizations for the securing and activation of deactivated authorization checks for authorization objects should be assigned to various users.
It is also recommended that the deactivation of authorization checks take place using the double-verification principle.

**CHECK FLAG IN SU22/SU24**

The following values are available for the check flag of authorization objects:

- **U** Check indicator not specified – authorization will be checked (as for ‘P’)
- **N** Authorization object check not executed by transaction
- **P** Authorization object check executed by transaction
- **PP** Authorization object check executed by transaction and the indicated field values will be suggested by the profile generator

The value “N” is subject to review and should be used only after close examination and documentation of test results. This value should be set only in the case where the organization can virtually guarantee that the object (and/or the application) will not be used.

**4.2.1.5.2 AUTHORITY CHECK FOR ABAP PROGRAMS (STANDARD SAP PROGRAMS OR CUSTOMER DEVELOPED)**

Access protection in SAP ERP Systems is essentially based on automatic checks located in programs. This involves the ABAP “Authority Check” statement, which can be included in ABAP program source code. When a program is run, the Authority Check checks whether the authorizations of the user who is calling the program are sufficient. If so, access is granted to the information; if not, the program must be configured in such a way that access is denied.

Reliable access protection can only be ensured if the authority checks are used correctly in the program source code. This applies to both standard SAP ERP programs and customer-specific reports.

It is recommended that programming guidelines that specify the details of what constitutes adequate programming, both technically and contextually, are developed. The “correctness” must be defined based on the existing authorization concept and data protection considerations.

**4.2.1.5.3 HR AUTHORIZATION SWITCH (TABLE T77S0: GRPID “AUTSW”)**

As described, the authorization object P_ORGIN (HR: master data) is significant with regard to access to personal information. Whether this authorization object and other HCM authorization objects or structural authorizations (switch ORGPD) are tested by the system depends on the Customizing settings. The settings are stored in table T77S0 (system table). In this table, semantic codes determine whether the authorization objects are active for authorization checks.

A complete procedure for the systematic check of assigned HCM authorizations, including the structural authorizations with the user information system, does not exist. The check at the single authorization level of a user can be completed with the transaction HRAUTH_Berechtigungs-Workbench (program: HRANALYSIS_TOOL) See SAP Note: 902000 - Analysis of HR authorizations. (So far no option for the reverse function exists: Who has which authorizations for an InfoType of a specific person?)
In order to reduce authorization check overhead, the exclusive use of the context-sensitive authorizations and the definition of critical structural profiles can be used effectively in connection with the appropriate authorization objects (PLOG_CON, P_ORGINCON, P_ORGXXCON) as “critical authorization” or “critical authorization combination”. Information regarding structure and function must be brought together and evaluated. For this the employment of third-party software (see chapter 6) is recommended.

### 4.2.1.5.4 REPORT AUTHORIZATION GROUPS

Access to sensitive reports can be protected by means of transaction code assignment or authorization groups in addition to the authority checks mentioned above. If the transaction code assignment method is used, it must be ensured that user reports can only be called via a specifically assigned transaction. In this case, it must not be possible to call reports via transactions such as SA38, SE38 or START REPORT (ABAP reporting).

Alternatively, protection may be implemented via authorization groups. Each relevant report should be assigned to a specific authorization group. Reports that are not used should be assigned to a ‘locked’ authorization group and generally accessible reports to a ‘general’ authorization group. Assignments can be made with report RSCSAUTH. The authorizations for the object S_PROGRAM (ABAP: Program Flow Checks) should be adequately defined in the authorization concept.

Because the SAP standard reports are normally delivered without assignment to an authorization group, this protective mechanism must be implemented at the user level.

For the reasons specified above, SA38 is to be assigned to users very restrictively. Each report which is not assigned to an authorization group can be implemented, without further checks28, with SA385.

### 4.2.1.5.5 RISKS AND MEASURES TO BE TAKEN

Deactivating authorization checks can be extremely risky, since this can disable the access protection mechanisms provided in the standard SAP System. In addition to checking the parameter AUTH/NO_CHECK_IN_SOME_CASES, the following procedures can be used for monitoring purposes:

- Display table USOBX_C (check table for table USOBT_C) using transaction SE17 (general table display)
- Analyze whether the table contains entries with OKFLAG = N. The authorization check for the relevant authorization objects is deactivated for specific transactions

Security measures against the global disabling of authorization objects (transactions AUTH_SWITCH_OBJECTS, SU25, SU26) are described in section 4.2.1.5.1.

As far as authority checks are concerned, the following measures form suitable starting points for ensuring data protection:

- Create development guidelines for programming customer-specific ABAP programs. These guidelines must stipulate, for example, how authority checks are performed, the authorization groups for reports, as well as test, release, and documentation requirements.
- Refer to the relevant SAP Notes (SAP Service Marketplace; http://service.sap.com/notes) for standard SAP ERP programs. Here, known problems and necessary changes are identified enabling Authority Checks in programs to be extended or corrected.

---

28 The Authority Checks in the program code, if they exist, will still be executed.
With regard to the HR authorization switch, the settings for the active authorization objects at the user level must be defined as target values. The actual settings made in the SAP ERP System (table T77S0) should be monitored at regular intervals. Furthermore, measures must be defined that prevent unauthorized users from modifying the program flag.

With regard to the report authorization groups, the authorization concept should define which measures must be taken to protect reports from unauthorized access. If authorization groups are used for this purpose, the assignments of reports to authorization groups should be monitored periodically. When a release is upgraded, note that new standard SAP programs must be included in authorization groups.

4.2.1.6 USER ADMINISTRATION

4.2.1.6.1 CENTRAL USER ADMINISTRATION CONCEPT

The user identifies himself to the SAP system by entering his user ID and his password. The user’s access rights are stored in the user master record. For storing this data, and for maintaining the access rights in the user master record, the SAP System offers various organizational alternatives.

In the case of central user maintenance, a central department is responsible for maintaining all the user master records. Roles and profiles can be assigned either centrally or locally (settings can be made via Customizing or at object or field level).

Since user administration and the administration of access rights can be problematic for security, the SAP ERP System offers the option to implement the multiple-verification principle.

This refers to the SAP recommendation to ensure a segregation of duties by establishing a user administrator, a roles administrator and an activation administrator, for example.

> The user administrator’s tasks involve creating and maintaining user master records.
> The role administrator maintains the authorization concept elements. Depending on the authorization concept, these elements are roles, profiles, or authorizations.
> The activation administrator is responsible for the usability authorization concept elements. The tasks involved here also depend on the authorization concept and include activating authorizations and profiles created by the role administrator in the maintenance version. They can also involve comparing users. In such cases, the roles containing the stored profiles and authorizations are assigned to the user master records.

SAP has defined the following authorization objects in the “Basis Administration” object class in order to enable the different administration tasks to be separated:

> User master maintenance: User groups (S_USER_GRP)
> User master maintenance: Authorizations (S_USER_AUT)
> User master maintenance: Authorization profile (S_USER_PRO)
> Authorization system: Check for roles (S_USER_AGR)
> Authorization system: Transactions in roles (S_USER_TCD)
> Authorization system: Field values in roles (S_USER_VAL)
> Admin function for user/authorization management (S_USER_ADM)
4.2.1.6.2 LOCAL USER ADMINISTRATION CONCEPT
With this form of administration, maintenance tasks can be distributed to several departments. The user group can be used to control which user master record an administrator is responsible for. Organizational responsibilities can be mapped in the system using corresponding authorizations for the authorization object S_USER_GRP (User master maintenance: User groups).

4.2.1.6.3 USER ADMINISTRATION WITH THE PROFILE GENERATOR
Roles contain the authorizations, with which a user can access the functions contained in the menu (transactions, reports/report, Web-supported applications, etc.). Roles are stored in the user master record.

With the tool for role maintenance (the profile generator) authorizations and/or profiles are automatically generated based on selected menu functions and then made available for editing. Furthermore, the profile generator offers integration with the HR organization management.

Unlike conventional user maintenance, time-dependent role assignments can be defined (temporary assignment of authorizations).

On the other hand, user master records can also be assigned to the roles. For this the transaction PFUD and/or the report RHAUTUPD_NEW (alignment user master record) are available.

4.2.1.6.4 OUT-OF DATE USER ADMINISTRATION WITH PROFILES
In the old user administration function, assignments in user master records took place directly through profiles (single or collective profiles). If the user administrator changed a user master record, the change took effect the next time the user logged on to the SAP system.

The use of manually produced profiles can lead to uncontrolled maintenance of authorizations.

4.2.1.6.5 RISKS AND MEASURES TO BE TAKEN
The risk associated with the user administration essentially entails unauthorized users accessing the SAP system and unauthorized, or too many, access rights for the user master records that have been created. This risk must be combated with organizational measures, such as the multiple verification principle and the technical implementation of these measures in the SAP system.

The authorization objects described in Section 4.2.1.6.1 are provided for this purpose. These objects can be configured for the relevant administrators to provide a segregation of duties as described above.

Since the segregation of duties with regard to the standard SAP profiles and roles is often taken too lightly
from a data protection perspective (see, for example, S_A.SYSTEM or SAP_BC_USER_ADMIN), company-specific solutions need to be created. The authorization objects named in 4.2.1.6.1 must then be configured in accordance with the resulting requirements.

If, due to the workforce available, it is not possible to divide functions into three levels (triple-verification principle), it is recommended that the functions be divided into at least two levels (user administration with role assignment and authorization administration with role and activation administration).

4.2.1.7 CHANGES TO THE PRODUCTION SYSTEM
Changes that are made in the production system are subject to the procedural logging requirements that are implemented for verification purposes. These requirements are found in Article 238 of the German Trade Law.

To ensure that changes are logged, various system settings must be made or basic protection mechanisms must be activated that prevent unauthorized changes from the outset.

4.2.1.7.1 CHANGE AND TRANSPORT SYSTEM

**DEFINITION OF CTO:**
The Change and Transport Organizer (CTO) provides functions for creating, documenting, and releasing change requests in Customizing.

**DEFINITION OF TMS:**
The TMS supports the organization and transportation of these requests.

As a rule, SAP recommends that three separate SAP Systems be used for application development and Customizing – a development system, a quality assurance system and a production system.

Consequently, due to …

> Maintaining the dataset protection,
> Protecting against unauthorized display of personal data, and
> Tracking changes to the system.

…authorizations for application development and Customizing should not be granted in a production SAP System. To configure the transport routes for the three systems above, administration authorizations are required (object S_CTS_ADMIN).

> Changes should generally first be made in the development system and transported into the quality assurance system using the TMS.
> Once an appropriate test, acceptance, and release procedure has been carried out, the changes are implemented in the production environment via the TMS.
> Depending on the configuration and dataset, personal data protected by the Data Protection Act can be present in all systems.

The implemented changes can be traced through the TMS logs.

The transactions STMS or SE03 can be used to examine logs of executed transports and changes.
4.2.1.7.2 TABLE LOGGING / CUSTOMIZING

When SAP is implemented and while it is in operation, a large number of tables are adapted to the requirements of the company.

Since changes to tables can generally be treated as program changes, any changes that have been made since production start-up must be logged. The table change logs must be kept for the statutory storage period (10 years).

By default, the delivered SAP system does not automatically log table changes, due to the extensive Customizing settings required.

The rec/client parameter is set to OFF for the test system. This setting must then be changed in the development system at the start of Customizing work and in the production system after production start-up by changing the standard profile (DEFAULT.PFL) so that either all table changes in the system (ALL) or at least the table changes in the delivery client (000), and the productive client(s) are logged. The ON setting is not permitted.

When the rec/client parameter is activated, change log records are written for those tables where the relevant indicator is set in the technical settings. Customers must, when needed, mark tables (T9, X, Y, or Z) they have created themselves to indicate that they require logging.

Table log indicators are maintained with transaction SE13.

In general, Customizing work should not take place in the production system. Instead, a test, acceptance, and release procedure must be carried out, in a different system, to ensure that the settings used are in line with the relevant requirements.

Note that when using the TMS, you must ensure that logging is also performed in the target system when Customizing changes are transported. In the configuration, the parameter RECCLIEN (parameter for table logging) must be set at the time of import (this parameter is not the same as the rec/client for table logging in the production system).

4.2.1.7.3 SYSTEM CHANGE OPTION

Transaction SE06 can be used to define whether repository objects and cross-client Customizing objects can be changed.

Individual objects, such as:
  > Customer developments
  > SAP Basis components, and
  > Development Workbench.
…specifically, can be protected. A button assigned to the transaction runs an evaluation of the relevant change logs.

The protection mechanisms established in this transaction do not affect the client-specific Customizing changes.
Appropriate protection mechanisms for these settings are configured by means of the client control settings (compare to “Protecting table T000”).

4.2.1.7.4 LOGS
When changes are made to objects/tables in SAP, an entry is created in a change log file, provided the relevant system settings have been made. This file is stored in the SAP file/database system. Each SAP installation has its own database and, therefore, its own file/database system. Exceptions to this are transport logs, which are stored in a shared transport directory.

4.2.1.7.5 PROTECTING TABLE T000: CLIENTS
By defining the relevant settings for table T000, general changes to the SAP System or in specific sub-areas can be prevented. Transaction SCC4: Client Administration is used to display and maintain the relevant settings.

Various settings can be made with regard to:
> Changes for transports and client-specific objects,
> Changes to cross-client objects,
> Protection of client copy and comparison/reconciliation tools.

In general, the settings should be defined in such a way that changes cannot be made in the production system.

If it becomes necessary to open the system with regard to change options, it must be ensured that no unchecked changes are made (corresponding documentation should be created) and that the change status is reset once the settings have been made.

4.2.1.7.6 RISKS AND MEASURES TO BE TAKEN
To ensure proper program use and to protect against unauthorized display or unintentional/intentional manipulation of data, it must be ensured that the system settings provide adequate protection against changes and that the necessary change logs are created. In this respect, it should be ensured that
> Clear and binding regulations are met with regard to maintaining, checking, and logging tables in order to be able to comply with statutory requirements, and to prevent the risk of datasets being manipulated purposely or inadvertently, as well as to meet the requirements for protecting personal data
> The relevant system parameters are set with respect to the TMS, transaction SE06, and the settings for table T000
> The logs created can be kept in accordance with the statutory storage periods and that, if necessary, they can be made readable again.

Regular checks of the settings made and downstream checks of the change documents are also necessary.

4.2.1.8 SYSTEM INTERFACES
SAP provides various interface methods for communication within an SAP ERP System, for exchanging information between different SAP ERP Systems, and for communication between SAP ERP and non-SAP systems.
4.2.1.8.1 BATCH INPUT
With the batch input method, data is saved in a batch input session. The data is then transferred by importing the batch input session. The batch input session simulates the online entry of transaction codes and data, and is subject to the relevant authorization and plausibility checks.

4.2.1.8.2 RFC, ALE, BAPI
Remote Function Call (RFC) is used for communication between distributed programs in an SAP System landscape. RFC can be used to call function modules in a non-SAP System and to return the results to the calling SAP ERP System.

RFC technology also forms the basis for other SAP specific interface methods, such as Application Link Enabling (ALE) and Business Application Program Interfaces (BAPI).

The hand-off of HCM data into a separate logistics system raises a special issue. SAP provides the option of passing the complete set of InfoTypes into the attached logistics system (see the transaction SPRO -> SAP Reference IMG -> SAP NetWeaver -> Application server -> IDoc Interface/Application Link Enabling(ALE) -> Modelling and Implementing Business Processes -> Configure Predefined ALE Business Processes -> Human Resources -> LO).

That means that during the transmission of the standard Infotype 0002 both the data fields “nationality” and “denomination” are transferred. These are data fields which, with high probability, cannot be legally processed in the logistics system.

Here it must be ensured through special measures in authorization management that misuse of this data is prevented (compare the appendix to §9, section 8 of the BDSG). Also, with other interfaces in HCM, such as Controlling or for the recording of hours worked (CATS and/or CATS XT), compliance with the permitted use of the data must be considered.

4.2.1.8.3 PC DOWNLOAD
SAP offers the option of transferring various evaluations by download from the “secure SAP environment” to the PC for further processing without any additional checks. The download function applies to the types of list outputs that can be transferred to the PC via the menu.

Menu path:
System → List → Save → Local file

Various authorization objects are provided in the SAP ERP System for combating the risk of personal data being transferred, and possibly misused, during processing.

4.2.1.8.4 ABAP LIST VIEWER (ALV)
The ABAP List Viewer, which is installed in many programs, enables displayed data to be transferred into any other program using the copy and paste functions, without being subject to any further authorization check or logging. See section 4.2.1.3.11.
4.2.1.8.5 RISKS AND MEASURES TO BE TAKEN

Following each data export into non-SAP systems, data usage rules, deletion periods, and other requirements of the Data Protection Act can no longer be ensured within the SAP environment.

For all types of interface processing, the main risks are:

> Incomplete or incorrect processing
> Manipulation during data transfer or the program run
> Unauthorized viewing of personal data
> Uncontrolled transfer of this data.

Suitable measures must be taken to combat these risks. As far as organizational measures are concerned, all interface files and the procedures used should generally be documented in accordance with the requirements described in the German Federal Data Protection Act (Article 4g, key word “Monitoring Proper Application” and Article 4e, key word “Describing the Data or Data Categories”).

As far as technical measures are concerned, different internal check levels are provided in the SAP ERP System, for which settings must be defined correctly (in particular in terms of the interaction between checks) and regularly monitored. The key technical aspects include the following:

<table>
<thead>
<tr>
<th>INTERFACE TYPE</th>
<th>RISK REDUCTION MEASURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>batch input procedure.</td>
<td>The authorization concept can define which users can create, process, and delete batch input sessions. Access is determined by authorizations for the authorization object S_BDC_MONI (batch input authorizations).</td>
</tr>
<tr>
<td>Remote Function Call technology (RFC).</td>
<td>Note the RFC destination security settings (transaction RSRSDEST – Output system overview for remote submit). These settings are maintained by the authorization object S_ADMI_FCD (system authorizations). The setting for the profile parameter auth/rfc_authority_check specifies whether authorization checks must be performed for the RFC. The parameter can be monitored by the report RSPARAM, et al. For security reasons, it is strongly recommended that the authorization check be activated for the RFC. If so, the access protection checks are performed using the authorization object S_RFC (authorization check for RFC access).</td>
</tr>
<tr>
<td>Application Link Enabling (ALE),</td>
<td>The distribution model and the ALE authorizations must be maintained. The transaction SALE can be used to access the relevant functions. The transactions and reports contained in this menu must then be protected accordingly.</td>
</tr>
<tr>
<td>PC download,</td>
<td>The authorization object S_GUI (authorization for GUI activities) is available for checking the generic download of lists.</td>
</tr>
</tbody>
</table>
### INTERFACE TYPE | RISK REDUCTION MEASURES
--- | ---
ABAP List Viewer | The relevant screen functions can be hidden in critical programs by making changes to the program, perhaps through the parameter IT-EXCLUDE in the REUSE_ALV_GRID_DISPLAY function component. The download authorizations for the transaction or the Report names can be controlled using User-Exit in user-defined source code.
Non-SAP solutions | Further SAP independent solutions can be implemented in special CITRIX environments, such as the blocking of the Cut-and-Paste function.

### 4.2.1.9 AUDITING AND LOGGING
The configuration and evaluation of the following logs, along with IT security, auditing and business audits, must be coordinated with the person responsible for data protection, and the co-determination rights of the employee representation board must also be observed.

For Auditing and Logging an operations concept is needed, in which the requirements for individual departments concerning the implementation, monitoring and storage periods are specified.

The necessary IT resource should be acquired (for example, additional storage needs).

#### 4.2.1.9.1 SECURITY AUDIT LOG
From a data protection perspective, it is recommended that users with extensive critical authorizations are subjected to compulsory logging using Security Audit Log. Since emergency users are equipped with comprehensive authorizations, it is legally required that executed activities be made traceable.

The required implementation of Security Audit Logs is to be viewed primarily in the context of operational safety and the data protection concept. Additional legal requirements must also be considered (e.g. GoBS, HGB, the Sarbanes Oxley Act).

The Security Audit Log is available as an “extended security log” in SAP systems. Using various filters uncritical, serious and critical events for the logging can be defined for different “audit classes”.

Transaction SM19 can be used to specify which events are to be logged for each instance, client, and user. Downloads can also be logged.

To use the Security Audit Log, the appropriate parameter values must be set. In SAP Note 539404, the most frequently asked questions about the configuration and application of Security audit Logs are answered.

To ensure that logs are actually created, in addition to the settings described above, the entry rsau/enable must be set to 1 in the profile parameters.
With the profile parameter `rsau/selection_slots` the number of filters (slots) to be available for the configuration of the Security Audit Logs can be specified. The system default value is 2. Starting with release 4.6, a maximum of 10 different filters can be configured.

Starting with SAP NetWeaver 6.40, the fields "user" and "client" can be set to generic values with transaction SM19. For the activation of the function the new profile parameter `rsau/userselection` was introduced, which can take the following values:

- 0 = generic selection disabled
- 1 = generic selection enabled.

The use of this option is recommended for situations where, for example, several emergency users are to be configured as a component of the emergency operations organization. By configuring a single shared filter, the activities of several emergency users can then be logged.

The use of general values has been available since the release of SAP NetWeaver 6.4, but is also available in older versions for certain Kernel patches. For more details, refer to SAP Notes 574914 and 59404.

The maximum size of the Security Audit Log file is defined in the profile parameter `rsau/max_diskspace/local` (default value = 1 MB).

The logs are saved daily to audit files by the Security Audit Log function. SAP recommends that these files be routinely archived and the original files deleted as needed. (transaction SM18).

When a high number of filters (slots) are activated, storage problems can occur. See SAP Notes 664058.

Transactions SM20/SM20N can be used to evaluate the logs created by Security Audit Logs.

**4.2.1.9.2 SYSTEM LOG**

The SAP ERP System generally logs different error situations in system logs (syslog at application level). These include:

- Logon attempts that lead to locking
- Processing terminations
- Miscellaneous problems and warning messages
- Use of the Replace function in the Debugger

The syslog can be called with transaction SM21.

If the Syslog is called, one can look for unusual activities and/or errors in the TCOD column using the search function (or other functions). For data protection purposes, transactions from areas such as PA and PD are of interest.

Syslog files are limited to a maximum length and when that length is reached the file is overwritten. For this reason the usefulness of Syslog is limited to checking clearly unusual system behaviour and/or violations of...
various regulations. Thus the organization should be instructed to routinely check the Syslog for specific messages or to increase the storage capacity of the Syslog (see SAP Notes 4063 and 548624).

4.2.1.9.3 TRANSACTION LOGGING STAD (CCMS)
SAP offers the option of logging all on-going activities via the CCMS (Computing Center Management System) for specific transactions and users on the application server. Statistical data can be created for each user on a daily, weekly, or monthly basis. (Transaction STAD and/or Report RSTAT 26)

The SAP authorization objects S_TOOLS_EX with field AUTH value S_TOOLS_EX_A and S_ADMI_FCD with field S_ADMI_FCD value ST0R are required for displaying statistical data on users.

Events that endanger security can be configured to appear as Alerts in the CCMS on the computer center console. The use of the transaction STAD and the system monitor STO3N (which makes the data for the STAD available) should be strictly regulated for data protection reasons.

4.2.1.9.4 WORKFLOW LOGGING
The Workflow component (SAP Business Workflow) provides tools for the automatic control and processing of cross-application workflow processes. Here it is possible to log all processing steps of the individual users (time of execution, duration, etc.) automatically. Tools available for this are, among others, the transactions SWU9 (display Workflow Trace), SWI2_xxx (Work Item Analysis) or SWI5 (Workload Analysis).

If the Workflow component is used, evaluation possibilities exist regarding user behavior (e.g. number of procedures executed). The use of this functionality, and its permissions, is to be submitted to a careful review related to data protection criteria.

4.2.1.9.5 REPORT LOGGING IN HCM
Downstream checks for starting “critical Human Resource Management reports” can be maintained in table T599R. The transaction SM30_V_T599 can be used to check which Reports must be logged.

If the implemented settings ensure that logs will be created, an evaluation can be carried out using report RPUPROTD.

From a data protection perspective, it is recommended that, at the very least, the use of flexible evaluations (such as reports RPLICO10 and RPLMIT00) and flexible absence evaluations (the RPTABSxx reports) be logged.

4.2.1.9.6 AD-HOC QUERY LOGGING RELATED TO “LIMITED USAGE”
The SAP system offers the option of logging the creation and execution of Querys for selected InfoSets (selection of InfoTypes and/or data fields from the HCM database).

The logging must be activated in Customizing with the transaction SPRO (→ SAP Reference IMG) → SAP NetWeaver → Application server → SAP Query → Logging → Determine InfoSets for Logging → ). The logged data can also be deleted here.
The logging records are written into the table AQPROT, which by appropriate measures and authorizations must be protected against manipulation.

The logging data can be evaluated using the user group /SAPQUERY/SQ and the InfoSet /SAPQUERY/ QUERY_LOGGING (in the global work area). The logs can also be conveniently displayed using the table display (SE17).

In view of data protection regulations, the use of query logging is recommended, if
> the adherence to the restrictions of data usage are in question (can occur when an InfoSet has a large number of data fields).
> a large number of users have the option of creating queries for the InfoSet in question.
> users with inadequately regulated rights, with respect to data protection regulations, have the option of creating queries for the InfoSet in question, and/or
> special data, as described in §3 section 9, is contained in the InfoSet.

In these cases it is advisable to continuously check whether adherence to the data usage rules applicable to the InfoSet are followed.

The Ad Hoc Query logging does not work for the other SAP Query tools, i.e. SAPQuery and Quick Viewer. However the SAP standard Queries can be called and logged using the functions of the Ad-Hoc-Query.

4.2.1.9.7 RISKS AND THE MEASURES TO BE TAKEN
For the issues described above, a distinction must be made between evaluations that enable downstream checks in the sense of an internal control system (ICS) and those that facilitate activity-related checks and, therefore, service and behavior checks.

If the workflow component, and to a lesser extent the syslog or the CCMS (STAD) is used, then evaluation options are available with regard to user behavior (for example, the number of activities processed, and so on). The use of these evaluations can be specifically restricted via the authorization concept. In relation to this, it is necessary to check the authorizations defined in the particular company. The AIS offers a good starting point for this check.

We regard the use of the security audit log to trace the activities of specially created emergency users as essential. This log represents an active component of a comprehensive security management concept. In this respect, it is important that a basic organizational framework be created above and beyond the technical measures described. This framework must ensure that the passwords of emergency users can be administered and reset, and the logs that have been created can be archived and checked.

4.2.1.10 COMPLEX SEARCH HELP
In SAP ERP complex search tools are available in different places. In many modules, such as HCM, they function as an internal information system. The available search assistance can be restricted using Customizing functions. The specification of the search function should take place in the project in consultation with the data protection officer and, if necessary, the employee representative.
TREX (text retrieval and extraction Machine), Knowledge Management (KM) and Search Engine Services (SES) create together an integrated enterprise-wide SAP search technology for both unstructured and structured data. The SAP search technology can be administered and monitored with different tools (TREX monitor in KM, TREX Admin Tool and TREX Alert Monitor).

In TREX a full text search through all documents in an electronic personnel document can be executed. SAP has built the TREX/SES functions into the e-Recruiting-application (administration applicant, etc.), for example.

From the data protection standpoint the use of this functionality, in particular relating to data usage restrictions, must be reviewed and regulated.

**DYNAMIC SEARCH AND DYNAMIC SELECTION**

SAP makes available for the administration of InfoTypes a search function which can access all data fields of all InfoTypes, but is not subject to logging.

The function also permits “dynamic selection” in Reports which permits access to the data fields of all InfoTypes and makes the Report results available, i.e. the selected personnel numbers. No logging for this function takes place.

The functions “dynamic search” and “dynamic selection” can be disabled and/or be restricted by limiting the search options and tailoring the operational requirements.

**4.2.1.11 SUMMARY OF THE KEY RISKS**

The following is an overview of the risks that tend to occur most often.

1. Not enough auditability and traceability/reproducibility due to
   a. Lack of documentation for customer-specific customizing and SAP System configuration (Customizing, table maintenance, application development, etc.).
   b. Neglecting to maintain report authorization groups.
   c. Careless handling of the authorization concept
   d. Ignoring recommendations (such as deactivated table logs, authorized programming in the production system, etc.)

2. Circumventing SAP ERP System access protections by means of programming options (in particular the Authority Check)

3. Circumventing SAP ERP System access protections by means of RFC-capable function modules that are called up from an unprotected SAP ERP System or from external programs

4. Misuse of the data via the download function and/or XXL List Viewer and subsequent processing of it for purposes prohibited by the Data Protection Act or under impermissible conditions (such as inadequate auditability)

5. Violation of the data protection requirements as a result of an inadequate authorization concept
   a. Violation of data protection requirements via additional analysis programs, such as: use of unapproved flexible analysis programs, ABAP reports, or queries (processing of data without a legal basis).
   b. Changing/Extending the scope of functions for originally approved programs/ABAPs/queries
c. The programming department accessing real data in the HR department
d. Programming of user-defined analyses using non-SAP approved, non-data protection compliant applications which can access SAP data (such as database tools not recommended in the SAP Security Guidelines)

6. Changing the system status, for example:
a. Granting access authorizations to an unauthorized user or for unauthorized programs
b. Configuring not agreed upon files, data fields, or data field value lists
c. Creating uncontrolled interfaces between personnel databases and other systems (such as controlling)
d. Improper configuration of the production system (for example, “changeable” status)

7. Misuse of data storage media, such as:
a. Analysis of data storage media containing personnel data at a different SAP installation (such as a service processing center) or on other PCs
b. Misusing backup copies

8. Concealing violations by changing system parameters by:
a. Falsifying log files, for example by temporarily deactivating table logging. This, however, requires access to the profile parameters, the table activation authorization, or the developer authorization
b. Circumventing the access authorization check by deactivating the authorization check

9. Circumventing the access authorization check and logging systems by means of PC download and analyzing data outside functioning security mechanisms.

4.3 SUMMARY OF THE CHECK PROCEDURES
In addition to the SAP topics discussed above, the following section discusses further checks that concern data protection requirements in more general terms. More information on these requirements is available in the general literature (see the bibliography in the appendix).

Implementing the necessary organizational and technical measures in order to meet data protection requirements and the ability to check the installation are the two essential requirements for processing personal data. The organizational and technical measures required must be examined individually by each user department for each form of processing and for each processing purpose when a system is planned (see the details in Section 1 of this guide).

Although a wide variety of compliance checks have been included here, there are others that have not been discussed.

Some of the issues not addressed in this document are checks of the principles of data reduction or data economy, the use of identity hiding (anonymization), the use of aliases (pseudonymization), and checks of processing reliability (the reliability of the “transfer of personal data to foreign countries” process, for example).

Such issues should generally be dealt with as part of the process compliance test run, that is, a one-time test of a program/procedure conducted before it is put into production operations.
In short, this means that the question of which measures are required or appropriate, or whether certain processing forms are allowed, must be examined on an individual basis.

In this context the following check list (see the “Checklist for the Requirements of Auditability” in Appendix 8.4.) is not intended to be a conclusive and exhaustive exercise, but is offered as a general guideline. The ultimate responsibility remains with the responsible organization.

In the checklist the various protective measures from this chapter are divided into three categories:
> Requirements related to auditability/transparency.
> Where necessary, separate technical-organizational requirements related to special security measures (e.g. customer requirements found in operating or service agreements).
> Requirements related to data protection measures in compliance with § 9 BDSG and the appendix for §9 BDSG.

The questions in the checklist have been written in a style that allows even casual users to gain insight into the system. The content refers often to the Audit Information System and its functions. For this reason, it is recommended that the SAP system audit documentation be available as a reference guide.
5 Order data processing and internal corporate data exchange

Chapter 5 deals with different forms of data processing orders, for example the assignment of one-time or on-going jobs to a Shared Service Center (internal or external), the creation of global processes with inter-company processing of personal data, or the use of external service providers (classical outsourcing).

Within each company or enterprise it must be established who the actual “owner” of the data is because, according to the BDSG, every legally independent unit must have a controller who can provide (perhaps in response to the information request of a data subject) information about data flows and the various employee subgroups with access rights.

In the 2009 amendment to §11 (2) in the BDSG, the controller is required to “verify compliance with the technical and organizational measures taken by the processor before data processing begins and regularly thereafter.” The result of this inquiry must be documented.

Failure to comply with both the stricter regulations in the recently updated standard contract for data processing services as well as the verification of compliance requirements are subject to penalties.

5.1 RESTRICTIONS ON OUTSOURCING AND DATA PROTECTION

In general, internal and external out-sourcing are treated differently.

For internal outsourcing the data processing is taken over by a legally integrated department within the responsible organization. From the viewpoint of the BDSG this data processing unit exists only for the purposes of this organization.

However, with external outsourcing the collection, processing and use of the personal data of the data subject takes place within a legally independent organization.

It must be determined on an individual basis whether a job is a data processing order as defined in §11 in the BDSG, or a take-over of the entire function (function transfer) in which the personal data of the data subject is transferred to the outsource service provider for independent collection, processing and usage.

Some examples of services that may be outsourced are:

> Outsourcing of the system/network administration and computer operations to another enterprise in the context of a service contract,
> Outsourcing of system preventive maintenance and updating to another enterprise,
> Outsourcing of system administration tasks and computer operations to various enterprises,
> Performance of tasks handling personal data by external service centers (Shared Service Center, Call Center),
> Transfer of the deployment of E-Businesses/Internet services to a Service Provider,
> Relocation of services abroad (European Union, European Economic Area, third world countries).
DEFINITIONS: DIFFERENCE BETWEEN DATA PROCESSING ORDER AND FUNCTION TRANSFER

Order data processing is characterized by the fact that customers and service providers - and this also applies to two companies within one enterprise - are separate, legally independent and self-employed enterprises.

The option exists, however, to view customers and service providers from a legal standpoint as one controller (see §3 (8) BDSG). This stems from the fact that the support provided by the service providers is simply the outsourcing of a procedure or the carrying out of specific instructions from the customer.

In this case the data collection, processing, or use, are simply outsourced as an auxiliary function that fulfils the tasks and business purposes of the responsible organization or customer.

To be considered legally separate, it must be the case that the service provider functions as a third party which may perform work that is outside the scope of the instructions provided by the customer/organization.

This will occur if the service provider performs additional processing, as determined by the service provider, on the personal data in question for the purpose of transferring or selling to another party.

Through the transfer of these tasks and functions to a third party the character of the data protection legal relation changes. The data involved in this relationship no longer serves the business purposes of the customer, in other words, data processed using the customer’s instructions, but rather that the service provider wishes to develop and produce, on their own, a specific contractually agreed upon outcome, for which they need this data.

In this case an entire function will transfer to the service provider, who will have sole responsibility for its performance. Thus a contract for delivery of services is awarded whose components are the collection, processing or use of personal data. The results of the processing are then made available to the customer.

This type of relationship is a function transfer.

The distinction must be made, using the criteria specified above for individual cases, between order data processing and function transfer in particular when tasks are outsourced to shared service centers or call centers.

In situations where the shared service center or call center completes the work using defined instructions, check lists, decision trees, or the work consists of simple transactions, the contract falls into the category of “order data processing”.

If, however, the service provider becomes the “owner” of the data within the context of the job accepted, allowing him to decide, for example, how the data will be distributed or how it is evaluated within the organization, then this is an instance of function transference.

When outsourcing occurs between two units in the same company, the legislation currently in effect should not be interpreted differently than it is between two independent organizations.

---

5.2 DRAFTING OF CONTRACTS BETWEEN SERVICE PROVIDERS AND CUSTOMERS

Due to the many questions related to aspects of contracts between customers and service providers, several basic points are discussed below. More detailed sources of information regarding data protection issues can be found in reference books (see Müthlein / Heck29 – in German). Much of the information in this section is taken from the Müthlein book.

The amendment to §11 of the BDSG in 2009 requires that the topics listed below must be addressed in contracts between customers and service providers (for more about changes to the amendment in 2009 see [GDD]30, for additional examples of standard contracts, e.g. see [Bitkom]31 and for supervision of data protection see [RP Darmstadt]) 32):

1. The subject and duration of the work to be carried out,
2. The extent, type and purpose of the intended collection, processing or use of data, the type of data and category of data subjects,
3. The technical and organizational measures to be taken under Section 9,
4. The rectification, erasure and blocking of data,
5. The processor’s obligations under subsection 4, especially monitoring,
6. Any right to issue subcontracts,
7. The controller’s rights to monitor and the processor’s corresponding obligations to accept and cooperate,
8. Violations by the processor or its employees of provisions to protect personal data or of the terms specified by the controller which are subject to the obligation to notify,
9. The extent of the controller’s authority to issue instructions to the processor,
10. The return of data storage media, and the erasure of data recorded by the processor after the work has been carried out.

It should be noted that in the public domain the federal data protection laws regarding contract drafts and information related to data processing jobs can have different requirements (in the sense of §11 BDSG). The country specific requirements for public organizations must be taken into consideration.

For particularly sensitive data, i.e. hospital and social security/insurance carriers, stricter regulations for outsourcing are applicable.

5.2.1 OBLIGATIONS OF CUSTOMERS AND SERVICE PROVIDERS

As the “data owner”, the customer is responsible for compliancy with the rules of the BDSG and other regulation concerning data protection.

In particular, the customer is responsible for the validity of the collection, processing and use of the data, for upholding the rights of the data subject, and for compliancy with respect to data protection legislation.

The service provider is obligated to choose, from among the technical and organizational measures offered, appropriate actions (commercial due diligence).

Written specifications describing the data collection, processing and use, technical and organization measures, as well as any additional sub-service provider relationships, are mandatory33.

---

30 GDD, Neue Anforderungen an die Auftragsdatenverarbeitung nach § 11 BDSG, Sonderbeilage zu RDV 5/2009
31 http://www.bitkom.org/files/documents/Mustervertragsanlage_zur_Auftragsdatenverarbeitung_v_3_0.pdf
32 http://www.rp-darmstadt.de/irj/RPDA_Internet?cid=cc0eeb29fc27e29ef6d7d34acc1c69e
33 See individual points in § 11 Abs. 2 BDSG
It must be confirmed that the instructions from the customer are followed. A detailed description of the data collection/processing/usage can often be waived when these aspects are already covered in a Service Level Agreement (SLA) with the service provider.

In addition to the tasks to be performed, SLAs frequently cover security issues such as availability, recovery or virus protection. In these cases, a reference to the data protection agreement in the SLA is sufficient.

The customer has the responsibility to ensure, as described in §11 (1) BDSG, that the service provider abides by the technical and organizational measures provided.

The scope of the inspection performed by the customer encompasses operational procedures, data processing systems and premises, and the confidentiality rules concerning knowledge of the data worked with.

The result of the inspection, which must take place before data processing begins, is to be documented. In addition, the schedule of subsequent investigations should be specified. The frequency is dependent on the sensitivity of the processed data. To simplify verification this document should be attached to the contract.

The contractor must confirm in-house that the data acquisition, data processing and/or data use follow the documented instructions and that technical and organizational measures are in compliance (with the appendix to §9 BDSG). The contractor’s employees are obligated to maintain data privacy.

The documentation of the procedures, to be transferred to the contractor, is to be created and maintained by the customer (responsible organization).

5.2.2 SCOPE OF THE DATA PROCESSING/INSTRUCTIONS
It is to be agreed upon what the scope of services will be, which databases (type, size) will be managed by the service provider and which procedures are to be applied to it (usually described in the SLA mentioned above).

Since the specific structuring of the contractual relationship can change, it makes sense to address those items which may change during the contract duration (such as change of personnel) in an appendix to the SLA or the data protection agreement.

Possible items to include are:
- Place, time and, when needed, the sequence of events for collection, processing and use,
- Procedures for data transfer (data volume, routing, encryption or other security measures),
- Authorizations and duties for the transport/sending of files, data storage media, documents or lists,
- Special requirements for the service provider (including authorized persons within the service provider team, contact person for the customer),
- Specification of the responsibility for archiving (data retention period) and deletion (see Chapter 2.3.5).

The contractual agreements can also be supplemented with instructions for individual cases. These can be put in an appendix in a pre-defined format.
At the same time, the instructions cannot exceed the rights of the parties in the specified contracts and must prohibit one-sided contract changes.

The contract provisions described by the BDSG relate to the handling of the data. As the data owner, only the customer has the right to write these provisions. If the customer wishes expanded decisional authority, this must be negotiated separately and specified in the contract.

Expanded definitions of the regulations seen in §11, No. 1 (data object and duration of the order) and No. 2 (scope, type and purpose of the planned collection, processing or use of data, the type of data and data subject description) are provided by the Bavarian State Office for Data Protection Oversight34 (Bayerisches Landesamt für Datenschutzaufsicht). These are:

1. THE DATA OBJECT AND DURATION OF THE ORDER.

**Specifics:**
- **Data object:**
  Payroll accounting, financial accounting, promotional mailings, call center services, telephone advertising, customer opinion poll services, closed circuit television services, Internet Providing, email accounts, data processing system support, maintenance/remote maintenance, data medium disposal, etc.
- **Duration:**
  One-time, valid until…, open-ended with option to cancel…

2. SCOPE, TYPE AND PURPOSE OF THE PLANNED COLLECTION, PROCESSING OR USE OF DATA, THE TYPE OF DATA AND DATA SUBJECT DESCRIPTION.

**Specifics:**
- **a) Scope, type, and purpose – processing or use of data**
  - Which exact services are to be provided (specifications, scope statement).
  - Order data processing only inland, within the European Union-/EWR-range or in third countries.
  - Which services will be carried out off-site.
  - Temporary or long-term storage of data by the service provider.
  - Which quantity of data, data records, data media.
  - Extent and duration of a closed circuit television service.
  - Use of telephone data or email addresses limited to traceable advertising promotions (proof of customer agreement to receive promotions)
  - etc.

- **b) Type of data**
  Personnel data, contract or order data, advertising data, advertising inconsistencies, survey results, health data, video recording data, use data from tele-media or telecommunication services, telephone call recordings, data processing logging data, etc.

---

c) Description of data subject

Employee, applicant, customer, prospective customer, supplier, advertising contacts, visitors/guests, passers-by, system user, etc.

An expanded definition of the regulations seen in §11, No. 9 (scope of the power to direct, held by the customer with respect to the service provider) is provided by the Bavarian State Office for Data Protection Oversight (Bayerisches Landesamt für Datenschutzaufsicht). This is:

Specifics:
> Specific instructions for order completion, (additional) security measures, and data protection violation response.
> Instructions for organization and/or completion of subcontractor relationships.
Who (on the customer side) gives the instructions and to whom (on the service provider side) are the instructions given to; how and in what form are the instructions delivered,
> etc.

5.2.3 TECHNICAL AND ORGANIZATIONAL MEASURES

In order to guarantee the exactness of the selection criteria the technical and organizational measures must be documented in a written contract, as described in §9 of the BDSG. This increases the transparency of the collection, processing and use, and facilitates inspections.

This type of description helps the customer’s operations DPO to comprehend his inspection rights with respect to the work of the service provider (§9 (6) BDSG appendix). In addition, it is helpful for the customer in cases where proof of liability related to the data subject is needed.

It is recommended that these measures be documented separately and referenced in the contract. This has the advantage that the modifications of the measures to bring them inline with the latest technical standard must only be changed in the appendix to the contract. Security measures which have already been included in the SLAs, do not need to be repeated.

When the outsourcing within the company has existing established security standard, a reference is sufficient. For details, various chapters of the data protection guidelines can be referenced.

An expanded definition of the regulations seen in §11, No. 3 (in relation to technical and organization measures seen in §9) is provided by the Bavarian State Office for Data Protection Oversight (Bayerisches Landesamt für Datenschutzaufsicht). This is:

Specifics:
For details see the appendix to §9 No. 1 BDSG, where the measures refer to specific situations, e.g.:
> Specification of transport routes and procedures for the data (manual, electronic) with appropriate security measures.
> Technical measures to guarantee reliability (secondary computing centre, emergency facilities).
> Procedure for the separation of the data of different customers.
5.2.4 PROTECTING THE RIGHTS OF THE DATA SUBJECT

The data subject has rights relative to the customer (data owner).

This means for the contract relationship, the customer must maintain control through the service provider of all necessary information and means for the protection of these rights to correction, information, blocking, and deletion.

The necessary support should be planned in advance.

An expanded definition of the regulations seen in §11, No. 4 (correction, deletion and blocking of data) is provided by the Bavarian State Office for Data Protection Oversight (Bayerisches Landesamt für Datenschutzaufsicht). This is:

Specifics:
- Co-operation of the service provider with requests from the data subject to the customer (see § 35 BDSG).
- Management of “no contact” lists for the customer (refusal to receive advertisements).
- Blockage or deletion of data according to special instructions or safe delete procedures.
- Deletion periods for closed circuit television data, for usage data from Internet or email providers.
- etc.…

5.2.5 DUTIES OF THE CONTRACTOR DESCRIBED IN BDSG, SECTION 11-4
(REQUIRED INSPECTIONS)

Concerning the regulations seen in Section 11-2.5 (duty of the contractor to make inspections) additional guidelines are provided by the Bavarian State Office for Data Protection Oversight (Bayerisches Landesamt für Datenschutzaufsicht). These are:

Specifics:
From BDSG, Section 11-4 BDSG the following regulations are relevant:
- § 5 BDSG - data secrecy
- § 9 BDSG - data security
- § 4f, § 4g BDSG - data protection officer

For example:
- Obligation of the persons employed by the service supplier to maintain data secrecy (including appropriate instruction) and appointment of a data protection officer by the supplier, name and contact information for the data protection officer.
- Inspection measures of the service supplier (internal revision, internal data protection officer, external auditing) for the adherence to data protection and data security, inspection reports.
Data Secrecy

For the employees of the service provider data secrecy (confidentiality), as described in §5 BDSG, applies to work activities involving the collection, processing or use of personal data in any of the phases of data processing (storage, transfer, editing, deleting or blocking).

In particular, the legal obligation to carefully choose the service provider requires that the contract addresses the confidentiality measures described above and how compliance with the requirements will be regulated.

Data protection officer of the contractor

In order to ensure that a competent contact person for data protection questions is available in the service provider firm, as well as to ensure that a “data owner” exists, the customer should have the name of the service provider’s data protection officer and should confirm that a change of data protection officers will be reported.

5.2.6 COMPLIANCE CHECKS PERFORMED BY THE CUSTOMER

To ensure that his contractual obligation to confirm compliance is met, the customer should list in the contract which compliance checks of the service provider’s work will be allowed, as well as how far in advance the planned checks must be announced. In addition the customer should, when necessary, in the contract reserve the right of review by a customer employee (for example, the operations data protection official) or by a specified third party. It should be noted that the omission of the examination before beginning of the processing carries a financial penalty.

Compliance checks can also consist of reviews of test reports or certificates produced by other institutions (e.g. by certified accountants or regulators). The data protection or confidentiality requirements of the service provider himself and his other customers should be taken into account.

An expanded definition of the regulations seen in §11, No. 2-7 (inspection rights of the customer and corresponding tolerance and cooperation duties of the contractor) is provided by the Bavarian State Office for Data Protection Oversight (Bayerisches Landesamt für Datenschutzaufsicht). This is:

Specifics:
> Scope of the inspection rights, with and/or without advance notice.
> The extent of the supplier’s obligations to cooperate and tolerate.
> Inspections at the service provider site, as well as sub-contractor sites.
> Who, on the customer side, carries out which inspections (departments, internal audit, data protection officer, external experts) and who works with the service provider (contact persons).
> Viewing rights of the customer concerning data processing logs, reports from internal audit and the service provider’s data protection officer, and external audits of the service provider.
> Viewing rights of remote monitoring screens.
> Inspection of the “opt-in” (agree to receive) advertising campaigns.
> Rights of access in private dwellings of telemarketers, etc.
5.2.7 SUB-CONTRACTORS
For individual areas of activity such as data collection, processing and/or use it may be necessary to bring in sub-contractors. These sub-contractor activities can include transport, destruction, collection, or archiving of data, as well as the delegation of work to backup computer centers in cases of high volume or system failures.

The conditions specified in the data processing contract between the customer and service provider should apply as well to the sub-contractor.

In the contract between customers and service providers subcontract conditions are to be specified. The corresponding sub-contractors are to be identified and their responsibilities with respect to the responsibilities of the main service provider are to be clearly described. In addition is should be stipulated whether the service provider has the right to negotiate with sub-contractors in the future. In this case, a procedure should be specified which requires the participation of the customer and is in compliance with §11 of the BDSG.

In addition it should be stipulated that, after agreement of all parties, the subject matter of the contract with the sub-contractor will be included in the contract between the customer and service provider.

An expanded definition of the regulations seen in §11, No. 2-1.6 (possible authorization for the formation of a sub-contractor relationship) is provided by the Bavarian State Office for Data Protection Oversight (Bayerisches Landesamt für Datenschutzaufsicht). This is:

Specifics:
For example,
> Subcontractor for which purposes, in which case, to whatever extent, also sub-subcontractor.
> Subcontractor agencies inadmissibly and/or under which conditions and after prior permission by the client permissible, designation of the subcontractors.
> Subcontractor only from the inland, also from the European Union-/EWR-area or also from third countries.

Not included in “data processing by sub-contractors” are so-called necessary additional services used by the service provider such as cleaning services, telecommunications services, maintenance work, etc.

5.2.8 SERVICE-PROVIDER VIOLATIONS WHICH MUST BE REPORTED
An expanded definition of the regulations seen in §11, No. 2-1.8 (service-provider violations which must be reported or data protection abuses or contract violations committed by its employees) is provided by the Bavarian State Office for Data Protection Oversight (government of middle Franconia). This is:

Specifics:
New regulations found in § 11 exp. 2 BDSG due to the new customer obligations seen in § 42a BDSG (duty to report illegal knowledge of data content).
For example,
> Which kind, which degree of offence must be reported (transmission errors, missing data media, misappropriated data, access authorization/password disclosures, etc.).
> Not only offences of the client and its employees, but also illegal actions of third parties (subcontractor, hacker, burglar).

5.2.9 RETURN OF DATA MEDIA AFTER PROCESSING
An expanded definition of the regulations seen in §11, No. 3 (return of data media after processing and the deletion by the contractor of stored data after completion of the order) is provided by the Bavarian State Office for Data Protection Oversight (Bayerisches Landesamt für Datenschutzaufsicht). This is:

Specifics:
> What is to return, and when, and what is to be deleted or destroyed (electronic data media, print-outs).
> Further use of electronic data media, etc.

5.2.10 PROCESSING ABROAD
With respect to data processing contracts negotiated with service providers within the European Union or the European Economic Area there is no difference between data processing carried out in Germany and processing carried out in other EU countries.

Based on previous interpretations of BDSG, for processing contracts with countries outside the EU the status of the data transmissions should be continuously communicated. This requirement has not been updated since the BDSG amendment of 2001.

This approach is, however, neither demanded by the European Union data protection guidelines, nor supported by subsequent communications of the European Commission, for example, through topics in the FAQ (Frequently Asked Questions) for Safe Harbor, or in the standard agreement clauses for data processing contracts with third countries.

The issue of data processing contracts with non-EU countries has also been addressed by data protection regulators, although with limited comments, in a resolution produced by the governing regulators for the private sector (Hamburg, Hillenbrand-Beck in RDV 2007, see page 231 and subsequent pages).

In an effective data processing contract the following points should be covered:
> It is to be determined whether a positive or negative decision of the European Commission exists regarding an appropriate protection level in this third country. This is valid, for example, for Switzerland, Canada and Argentina.
> If necessary, the European Union standard agreement clauses can be used at the basis of the contract.
> Through individual clauses in a contract, authorized by the regulators, sufficient guarantees can be specified.
> In § 4c BDSG exceptions are mentioned, in which transmissions to third countries are permissible if an appropriate data protection level is not ensured. Examples: If the data subjects have consented or a contract with the data subjects exists. In all cases, the restrictions on use of the data should be described in the contract.
In the USA enterprises can “self-certify” themselves to the Safe Harbor framework. These US companies want to guarantee an appropriate data protection level (EU approved) by adherence to these regulations (www.export.gov/safeharbor).

The regulation in §11 exp. 2 BDSG means that the customer must make sure that the work performed by foreign service providers meets these technical and organization measures.

Due to the specifications of the BDSG regarding, in particular, the naming of a data protection official in the service provider’s organization, as well as the confidentiality obligation, it will be necessary to adapt the contents of a standard agreement for data processing contracts.

Instead of naming a specific data protection official, the service provider should name a person responsible for assigning data protection officials as needed.

The obligation described in § 5 of the BDSG can be replaced by a similarly worded customized version of the duties of the service provider’s employees.

5.2.11 MAINTENANCE AND SERVICING

By definition the regulations related to data processing contracts in the sense of the Federal Law for Data Protection are to be applied, in accordance with §11 paragraph 5 BDSG, to the performance of maintenance work or of comparable support services if in the performance of these services an access to personal data cannot be excluded.

The maintenance and servicing of systems may include some of the following activities:

- Installation and servicing of networks, hardware and software, among other things (operating systems, middleware, applications)
- The setting of software parameters
- Program development/adaptation/conversion
  Execution of migrations in the production system
- etc.

Maintenance activities can be carried out on site or remotely.

The maintenance activities for SAP system operations can involve all levels of data processing operations including hardware, operating systems, databases and networks.

For this reason, system and applications data can be affected, although only applications are of interest when considering personal data.

Consequently, the BDSG differentiates between maintenance activities. These requirements need only be of concern if the maintenance of application data extends to personal data.

In all cases it is incumbent upon the customer to approve and check maintenance activities related to individual cases.
Regarding the protection of personal data in relation to unauthorized access and/or further use by external system attendants/maintenance staff, suitable safety precautions must be provided:

> The type and scope of maintenance are to be agreed upon in writing.
> The maintenance staff should also sign an agreement to protect confidentiality. This applies equally to staff performing remote maintenance work (“remote access”).
> Personal data in the productive system may not be downloaded to other systems.
> For maintenance activities performed via Remote Access, the “principle of least privilege” should be utilized. Access to computers and applications in the production system can be granted as needed.
> The system administrator has the responsibility to ensure that all system side maintenance procedures to programs and databases are promptly and properly logged.
> Maintenance staff should have no direct access to personal data (through the use of separate partitions, for example). In an emergency situation where personal data is accessible, the system administrator must provide appropriate measure for monitoring maintenance (including remote) personnel, which may include being physically present.

Within the framework of routine, systematic maintenance tasks using remote access, which is used frequently to update system environment, access rights should only be granted by the customer’s system administrator when specially requested by the service provider.

SAP has created a security concept for these types of maintenance activities and will provide them to customers upon request.

5.3 SAP FACTS

5.3.1 INITIAL/STARTING SITUATION

The outsourcing of data processing functions to third parties (so-called order data processing – see §11 BDSG) is a frequently occurring special case of the BDSG as well as in SAP operations.

In the sense of the BDSG customers and service providers are regarded together as a single “controller” or customer. In this relationship, the service provider is subject to the instructions given concerning the collection, processing and use of the data. The technical/organizational measures, however, are subject to the terms of the contract.

The service provider, on the other hand, is responsible for informing the customer when the customer’s instructions are not in compliance with the requirements of the BDSG.

SAP ERP is a multi-client system with overlapping cross-client and cross-company functions, with whose assistance both complex company structures and several independent enterprises in a SAP system can co-exist.

In the case that the enterprises are independent of each other and no need for consolidation exists, it is recommended that separate systems are used, and at a minimum, separate clients.
5 Order data processing and internal corporate data exchange

In the last case care should be taken that employees of the controller do not grant cross-client authorizations (e.g. no client-independent table access, no system authorizations).

With particularly sensitive data such a separation may be required. A separation into accounting areas (company code) is provided within corporations. Here it is to be made certain that the access rights reflect the legal restrictions of the corporation.

Deviations from this must first be negotiated between the separate companies to conform to data protection recommendations, then given to the service provider.

An additional separation within plants and/or Human Resources is not legally mandatory with respect to data protection. A separation here is related more to wage and work time provisions. Regarding the privacy of personnel data an appropriate restriction of authorizations is recommended.

Because the BDSG does not address data protection at the corporate level, from a data protection perspective the focus of secure data processing must be at the company code level as it is the smallest legally independent unit with its own balance sheet.

The range of data processing tasks transferred to the service provider will naturally vary depending upon the job order.

For example, the customer can, in addition to computer operations (deployment of SAP systems), more or less outsource the enterprise-specific servicing of the SAP applications, Basis systems and the operating system components to the service provider.

Due to the fact that computer service centers are, as a rule, handling various customers, the service provider must take special care, with respect to access prevention mechanisms, that personal data of different users are treated confidentially and kept separate.

5.3.2 SAP ADMINISTRATION
Control of the authorization administration (defining who may do what with which data and which functions) must remain with the customer. On the other hand, the system administration is a task of the service provider (an exception may be the use of a system with a productive client). However, access to the controller’s personal data by administrators must be regulated within the context of the work order.

SAP specific tasks, competencies and responsibilities (e.g. SAP users, authorization, activation administrator, SAP System administrator, etc.) should be clearly specified in an attachment to the contract.

The authorization objects,
> „User master care: User groups“ (S_USER_GRP)
> „User master care: Authorizations“ (S_USER_AUTH)
> „User master care: Authorization profile“ (S_USER_PRO),
…are to be adapted according to the agreements with service provider and/or customer.
This also applies to the establishment of a technically competent operator organization (for further information about authorization objects and profiles see chapter 4).

5.3.3 SAP SPECIFIC MEASURES
In the case of contract data processing the technical and organizational measures seen in § 9 BDSG and their SAP specific characteristics (see chapter 4 implementation of the requirements out of § 9 BDSG and appendix: Technical-organizational measures) are assigned a special meaning since they concern, under certain circumstances, separate scopes of responsibility.

The following points are of particular importance:

5.3.3.1 SYSTEM ADMINISTRATION
It is to be examined carefully, to which extent comprehensive and/or far-reaching authorizations and/or roles are assigned to employees of either the service provider or the controller. There may be a risk that cross-client and cross-company code functions can be exploited.

For example, under certain circumstances, personal data in accounting area “xxxx” can be accessible to users in accounting area “yyyy”.

On the other hand, it is to be examined carefully to what extent administrators of the service provider receive access rights to personal data of the customer.

System administrators are to have no authorizations on the productive client of the principal (exception: Client 000 and, if necessary, 066). For emergencies a special emergency user is to be defined by the customer and temporarily activated.

5.3.3.2 CHANGE AND TRANSPORT ORGANIZER (CTO / CTS)
If SAP application development and/or the authorization for changing development objects is outsourced to the service provider, it is to be guaranteed that test data (frequently this concerns original data of the productive system for integration tests) is made available only to the legally independent units (accounting areas) and/or to contracted third-parties.

In principle, in order to ensure the security of the databases, to prevent unauthorized knowledge of personal data and to maintain the traceability of bookkeeping, the authorization for application development in a production system may not be granted.

If emergency users with these authorizations exist, it must be organizationally ensured that all activities of these users are documented in detail. The Security Audit Log can be used to log the activities of emergency users.
5.3.3.3 REMOTE MAINTENANCE UND SERVICES

Maintenance and servicing activities via data line take place in SAP systems for functions such as:

- SAP EarlyWatch check
- Going Live check
- SAP Upgrade Assessment

Because access to SAP and the performance of these functions within contract data processing are on an equal footing, appropriate rules governing the type, scope, and permissibility of the service activities must be formulated. SAP provides the document “Security and Data Protection at SAP” to customers upon request.

The user Earlywatch is the dialog user for the SAP EarlyWatch Check in the client 066. It is needed only for the Performance Monitor. This procedure runs, as a rule, only at the request of the appropriate company. In principle this user should not have the profile SAP_ALL because it includes the rights to perform maintenance on cross-client tables. For this reason activity-related roles should be provided.

For the protection of these users from unauthorized access the initial passwords are to be changed. In addition, technical and organizational measures should be put into practice. This guarantees that only those functions which are intended for the use of these users are implemented.

An option for checking the SAP measures carried out by the Earlywatch user is to use the Security audit log. Further it is recommended that this user is activated only in accordance with a written procedure.

5.3.3.4 RFC AND ALE

The remote Function call (RFC) serves as the communication between distributed programs in a NetWeaver based system landscape. Using RFC, functional modules in an external NetWeaver based system can be called and the results will be returned to the calling NetWeaver based system. Other NetWeaver-based specific interface methods such as Application Link Enabling (ALE) and Business Application Programming Interface (BAPI) are based on the RFC technology. If external systems are connected, or service/maintenance is performed using RFC, the functions to be executed must be identified. This is particularly important when data processing is performed by third parties. Additional technical, as well as organizational, measures are to be taken, by which it is guaranteed that the BDSG appropriate data protection level will be maintained.

5.3.3.5 JOB HANDLING

Between customers and service providers the responsibilities related to job order, job execution, and job monitoring must be clearly defined in writing (e.g. payroll run, dunning run). These procedural instructions should be made available to both the customer’s departments as well as to the EDP managers of the service provider. The job logs generated in the SAP system show the parameters used for the job. These logs should be protected – normally by the contractor. The minimum retention period for job documentation according to commercial law is 10 years, and must be accessible for the data protection officer during this period. The confidential handling of print-outs containing personal data for the respective legally independent units must be guaranteed.
5.3.3.6 PC DOWNLOAD
The transmission of SAP data from “the secured SAP environment” by PC download can be prevented starting with version 4.0 using the authorization object “authorization for GUI activities” (S_GUI). In releases starting with 3.0C downloads can be prevented and/or logged using download functional modules (see SAP Notes 28777 - “PC Download: Logging, authorization check”). On a PC a user can copy data using “Cut and Paste”. For this situation the contractor must create suitable organizational controls which prevent the usage of personal data without knowledge of the customer.

5.3.3.7 DATABASE AND LAN ENVIRONMENT
SAP provides in the SAP NetWeaver Security Guide basic recommendations regarding the installation of the database and the network. For a date processing order it must be determined whether the customer should install their own client or system.

5.3.3.8 CROSS-CLIENT FUNCTIONS
When copying clients between two systems, e.g. with the transactions SC1 (using transport request), SC9 (remote) and/or SCL (local), corresponding care is to be used by the service provider. If necessary, appropriate instructions should be provided by either the customer or the service provider. This also applies, of course, to the use of transaction SC5 (delete client).

5.3.3.9 SAP LOGS
The contractor must keep, for data protection and liability reasons, archived SAP logs as proof of the execution of the data processing. This is important for both contractual stipulations and possible follow-up audits.

The job inspection can cover job logs, schedules, special work verification, orders for customizing, transport requests, etc.

The retention periods could follow the commercial and tax law regulations.

It should be noted that, to some extent, logs do not permit a customer specific evaluation.

This applies in particular to log files if the data of several customers are processed on the same system, in the same client or in the same organisational structures (company code, plant/personnel area, etc.).

In order to distinguish between jobs to be evaluated it may be necessary to implement additional filters. These filters are not available in standard SAP.

This type of filter could, for example, use the user identifications of the customer.
5.4 RISKS
If personal data are processed or used by a third party in a contractual relationship, the danger exists that the data processing service provider may not sufficiently meet the data protection-legal requirements or comply with contractual agreements.

In the long run, however, the customer’s executive management is responsible with regard to the data subjects and the supervisory authorities.

Due to these circumstances, the customer is obligated to make sure that data protection regulations and contractual provisions are adequately complied with. At the same time the service provider is obligated, with respect to data protection, to ensure the careful handling of personal data from different customers (SAP users) and to prevent the unauthorized transmission of such data.

The service provider is, to that extent, responsible for the appropriate organizational integration of the SAP systems used for processing of personal data in their own internal control system.

With respect to order (contract) data processing, fines can be imposed on the customer for the following violations (§ 43 exp. 1 No. 2b BDSG):

To deliberately or negligently violate…

> BDSG, Section 11-2.2 by awarding a contract that is incorrect, incomplete, or not in the legally prescribed format

> BDSG, Section 11-4 by not ensuring before the beginning of data processing that the contractor/service provider will adhere to the technical and organizational measures agreed upon.
6 Special Topics

6.1 AUDIT TOOLS: AUDIT INFORMATION SYSTEM AND USER INFORMATION SYSTEM

6.1.1 AUDIT INFORMATION SYSTEM (AIS)
The AIS is designed as a tool for the auditing of SAP system and is used primarily by quality system auditors, internal auditors and external auditors. It is supplied in the standard scope of SAP ERP and leads, according to the documentation, to “an improvement of the audit quality and a stream-lining of the audit process flow”. The AIS contains a collection, structuring and pre-configuration of audit functions including documentation, audit standard reports and download of audit data.

In principle the AIS is divided into the areas of business audits and system audits. The business audit contains, in addition to organizational overviews, balance sheet oriented and process-oriented functions. This permits, for example, the examination of information about customers, vendors, financial accounting and tax interests.

The audit system of the AIS is subdivided into different areas: among other things, general system checks, analysis of the users and authorizations as well as the audit of the repository and the tables. In this way it offers an auditor extensive functions for the inspection of the system status, such as system parameters or the transport system.

One of the tools available for the analysis of a SAP authorization concept is “Infosystem Users & Authorizations”. This program can be sued to create various standard reports about users, roles or change documents (logging of the user and role administration).

The AIS also offers, however, assistance to the Data Protection Officer with his tasks. This assistance can help in particular with…
- data protection audits (see chapter 2.1 and 4.3)
- information requests from data subjects (see chapter 3.1)
- the creation of overviews (see chapter 2.3)

The AIS offers the following standard reports for the creation of overviews (according to §4 BDSG, file register):

- Where-used list of domains for non-empty database tables
  - File register for employee data
  - File register for applicant data
  - File register for vendor data
  - File register for customer data
  - File register for partner data
  - File register for accounting clerk data
  - File register for sales group data
  - File register for patient data
  - File register for R/3 users.

The AIS was changed (since Release SAP 4.6C) from a menu structure to a role-based maintenance environment. Every AIS user needs roles, based on his tasks, which are stored in his user master record.
SAP delivers 71 standard roles for the work with the AIS (Selection SAP*AUDITOR *).

An overview of the AIS standard roles, relevant for the Data Protection Officer, is found at the beginning of chapter 2 (Tasks of the Data Protection Officer). Also provided are recommendations for the role assignment to the DPO as well as additional references.

More information can be found in the documentation for the Audit Information System as well as the SAP Notes 754273 and 451960.

However, the AIS is no longer current with regard to data protection. For years the data protection functionality in the AIS has not been maintained or improved by SAP. This can be seen in the use of obsolete terminology (such as “file registers”). Further evidence is the lack of interest on the part of SAP in further development of the AIS.

Members of the DSAG (data protection working group) detailed in September 2005 requests for the improvement of AIS in the data protection menu option:

> The previous function for the “file register” must be adapted to the usage of the BDSG and extended to further domains where personal information is stored (for example EKGRP).
> Functionality for the display of data of a special kind should be offered for the support of a pre-production compliance check of automated procedures.
> It should be possible to display the “life cycle of personal data” in order to evaluate, for example, the duration of the retention period or to determine whether the purpose of the data collection is still valid.
> A function for the “data confidentiality obligation” should exist (infotype “Company Instructions”).
> A function for the distribution of information to employees (up to now: in the session “HR data, function, infotype overview of an employee”) should be integrated into the “Data protection” menu option.

These suggestions for improvement refer not only to data protection but also to the functionality for Human Resources (HCM), to the analysis of authorization concepts and system status, as well as to the logging options in ERP SAP.

It is currently unclear which strategy SAP is pursuing with the AIS. Whether and how further development will occur, or whether other Tools are planned to replace the AIS, is not known.

6.1.2 USER INFORMATION SYSTEM (SUIM)
The User Information System (transaction SUIM) can be used as an analysis instrument for the authorization concept of an SAP ERP system. It helps the auditor to acquire an overview of user maintenance, for example, using…

> the users and their access authorizations
> the roles, profiles and authorizations available in the system
> the authorization objects defined by SAP, as well as
> all change documents (logs) for users, roles, profiles, etc. 36

---


36 For the use of the User Information System compare the relevant SAP Notes, as well as section 4.2.1.4.5 (Role with critical authorizations): “Depending on the quality of role maintenance, the SUIM can be misleading.”
With the User Information System up to now, however, only the authorization concept of the "classical ABAP world" can be analyzed. The authorizations assigned within the framework of the Java environment (for example, for portals) and the so-called “structural authorizations” cannot be checked with the User Information System. In special SAP systems, as in “CRM SAP – Customer Relationship Management” for example, additional tools for authorization management are provided when needed (cf. “Data Protection User Guide for CRM mySAP, section 2.5.2”).

It would be advantageous if SAP integrated this type of functionality into the User Information System and documented existing functional gaps.

6.2 SOS-REPORT (SECURITY OPTIMIZATION SERVICE)

SAP makes available, and now for the customer automated and free, a remote service (ST14: Application analysis > Security Optimization). This service analyzes the security settings for the ABAP stack and carries out an evaluation of risks presented in traffic light form. Its set-up is similar to the EWA service (Early Watch Alert) and it identifies high, middle and minimal risks (according to the SAP definition) to ensure a secure system operation.

The SOS Report is produced on the active system. It is made available to the SM System (Solution manager) integrated into the SAP system group for formatting, viewing, as well as processing (SM transaction: Solution_Manager). It can also be periodically requested and retrieved from the SM System.

The report supplies, using the familiar SAP Report format, a great number of standard reports out of the User Information System for critical authorizations from all of the usual security settings areas. Some examples are: system and client settings, user administration, logon, Security Audit Log, selected HCM authorizations.

SAP administrators or users with high departmental/technical administrative rights can be entered into a Questionnaire and thus excluded from lists and risk-related valuations.

The SOS Report supplies a good overview of the individual security settings of the ABAP stack. At the same, it provides a standard for the division of labor and responsibilities for tasks critical to security and the relevant required authorizations. An example of this is the display and query concerning the use of the SAP_ALL profile in the system. The issues of which authorizations are truly needed or actually available are clearly presented.

The Security Optimization Service provides an orientation for the security status of SAP operations. This service should be used as a method for determining whether the level of protection based on technical measures, revealed in the operations security and risk analysis, has been implemented and maintained.

The service is available only in the English language. Additional information can be found in the SAP-Marketplace (http://service.sap.com/sos).
6.3 SAP GRC (GOVERNANCE, RISK AND COMPLIANCE)

The SAP GRC Suite contains solutions for risk management, for the documentation of the internal control system, for access and authorization management, as well as for global trade and environmental, health and work protection.

The use of the applications for Governance, Risk and Compliance decreases the effort required to comply with important rules and legal requirements, and increases the transparency of enterprise-wide risks.

The use of the GRC Solutions software requires SAP NetWeaver integration and application.

The GRC Suite consists of, among other things:
> SAP GRC Access Control, Access and Authorization Control
> SAP GRC Process Control, Solution for the documentation of the internal control system
> SAP GRC Risk Management, risk identification and analysis

Furthermore, additional GRC Solutions guarantee the observance of regulations in numerous industries.

### SAP SOLUTIONS FOR GRC

#### INDUSTRY-SPECIFIC GRC

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Process Control</th>
<th>Global Trade</th>
<th>EH&amp;S</th>
</tr>
</thead>
</table>

#### CROSS-INDUSTRY GRC

<table>
<thead>
<tr>
<th>Risk Management</th>
<th>Access Control</th>
<th>Process Control</th>
<th>Global Trade</th>
<th>EH&amp;S</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>SAP NetWeaver</th>
<th>BUSINESS PROCESS PLATFORM</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>BUSINESS APPLICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP</td>
</tr>
</tbody>
</table>

The applications in the SAP GRC Suite are additional software not available in standard SAP. A license for the use of this software must be purchased from SAP.
6 Special Topics

6.3.1 SAP GRC ACCESS CONTROL

SAP GRC Access Control manages the access and authorizations in real time. The application analyzes and evaluates risks on the basis of current data and can thus immediately recognize conflicts related to segregation of duties and critical accesses.

Before authorizations are assigned, a risk simulation can be run in order to uncover potential infringements.

The segregation of duties is enforced through the use of an extensive database of rules appropriate for ERP systems. The authorization concept is analyzed on the basis of these rules. Access Control analyzes the access controls throughout the enterprise in ERP systems for SAP, Oracle, PeopleSoft, JD Edwards and Hyperion.

The implementation of Access Control occurs in several steps.

The first step consists of the identification and elimination of risks in access management. Within the business applications critical transactions and conflicts with respect to the segregation of duties are recognized by means of rules (risk analysis and remediation). After that, the role definitions and administration, with the aid of Access Control (Enterprise Role Management), are standardized and centralized.

Critical authorizations are then removed from the actual roles using an access control for superuser or privileged user (Superuser Privilege Management).

When role definition and administration is centralized, secure processes are defined using Access Control (Compliant User Provisioning) for rule-consistent role assignment. In addition, it will be determined for this purpose whom within the Workflow is to be informed of requests for authorizations. If these persons give their approval, the role is assigned automatically to the requestor.
The use of SAP GRC Access makes the evaluation of the authorization concept considerably easier for the Data Protection Officer because it is not necessary to evaluate every authorization object or transaction separately. It is also possible to define rules (for example, for P_ORIGIN) or to classify transactions as critical (for example, PA30). The data protection problems associated with emergency users, in particular, are resolved in Superuser Privilege Management.

6.3.1.1 RISK ANALYSIS AND REMEDIATION (PREVIOUSLY “COMPLIANCE CALIBRATOR”)
Risk Analysis and Remediation makes it possible to discover critical transactions and conflicts with respect to the segregation of duties within roles or profiles. A “Rule Set” with rules for the segregation of duties in the ERP systems of SAP, Oracle and PeopleSoft, JD Edwards and Hyperion is compared in real time with the available authorizations.

In this way Risk Analysis and Remediation automatically recognizes existing and potential risks in access control. In addition, rules can be defined or critical transactions identified.

Standard reports for the evaluation of risks based on users, user groups, roles, profiles and critical transactions are provided in the application.

With the help of Risk Analysis and Remediation…
> it is determined whether a collection of authorizations and activities of a user, a role or a profile contain risks,
> it is determined whether risks arise when additional activities, roles or profiles are assigned to a user (Simulation),
> an alert is generated if a critical transaction is executed.

An important component of data protection is the control of access to data, the use of critical transactions and, in HR, the access to infotypes and subtypes. Through the precise definition of the access risk and their storage in the system the risks related to roles and users can be evaluated.

6.3.1.2 ENTERPRISE ROLE MANAGEMENT (PREVIOUSLY “VIRSA ROLE EXPERT”)
Enterprise Role Management centralizes and standardizes the installation and administration of roles in the organization. Managers can define roles based on functions while IT administrators define the corresponding technical authorizations. Through flexible process mapping and automated hierarchical role generation it is simple to create and maintain roles.

The application in this way reduces the danger of errors and facilitates the consistent implementation of proven procedures.

Enterprise Role Management is integrated into the profile generator, therefore roles once defined can be generated automatically in SAP system.
6 Special Topics

6.3.1.3 SUPERUSER PRIVILEGE MANAGEMENT
(PREVIOUSLY “VIRSA FIREFIGHTER FOR SAP”)

Superuser Privilege Management makes it possible for users to execute emergency measures which are outside of their usual roles. This occurs in controlled surroundings and with transparency for internal audits. A temporary user profile (Superuser-ID) is assigned to the user. This permits, for example, critical transactions access or extensive system access.

The application can observe, monitor and log every activity and use of the Superuser-ID. Managers receive an automatic announcement about the use of the Superuser-ID and the corresponding log files. It is determined in advance which users are assigned a Superuser-ID in order to avoid hesitations in emergencies.

6.3.1.4 COMPLIANT USER PROVISIONING
(PREVIOUSLY “VIRSA ACCESS ENFORCER”)

Compliant User Provisioning facilitates the proper granting of access rights. Dynamic workflows automate the approval process in which every request is passed on to the responsible persons (for example, by e-Mail). These persons are informed of authorizations already available to the requestor (and if needed, potential risks arising through additions) and can then agree or refuse. If an approval is given, the role is created automatically, provided that it was defined previously with the help of Enterprise Role Management.

In addition, users can use Compliant User Provisioning to reset their own passwords.
6.3.2 SAP GRC PROCESS CONTROL

The SAP GRC Process Control 2.5 application (Process Control) is used for the documentation of the internal control system. Process Control supports the execution and monitoring of controls with respect to business processes and the company-wide IT infrastructure. In this way documentation, evaluation and testing of the controls, as well as the control and monitoring of control vulnerability elimination is supported. This will ensure that regulations for financial reporting, such as those in the Sarbanes-Oxley Act, will be followed.

The structure of the organization can be shown in an organization hierarchy. Processes and sub-processes are defined for the entire organization. Controls which cover risks can be assigned to a process or sub-process.

The controls can be evaluated regularly through scheduled test runs. Within Process Control the controls are divided into automatic, semi-automatic and manual controls. SAP delivers automatic controls starting with Process Control 2.5.

Within the application user-designed manuals and semi-automatic controls for the processes can be defined. For this purpose queries can be created, or Reports (SAP standard programs and customer programs) scheduled which Process Control starts automatically on the ERP system. The results are then passed on, in Workflow, to the responsible user evaluation.

The status of the controls, tests, processes and organizations can be frozen by executing a Sign-off. In this case the responsible users must confirm the documentation of the processes and the effectiveness of the controls. It is possible to examine the status of the Process Control master records at a specific point in time and to recognize differences between various points in time.

Within the framework of data protection Process Control can be used to define and document data processing processes. In addition, making detailed instructions and approved templates available simplifies manual audit tasks for employees.

This ensures, among other things, that...

> the rights of the employees concerning personal data are preserved
> the compliance with data retention periods can be checked and database reorganization is transparent,
> the legal requirements for data processing orders will be met (documentation, requirement checks)

In cases where checks uncover discrepancies or processes have been changed, the Data Protection Officer (and/or the responsible employee) can be automatically informed (via Workflow).
7 SAP Websites

http://help.sap.com/

http://www.sap.info/de/glossary/A.html


http://service.sap.com/alm-methodologies
(Accelerated SAP, ASAP Implementation Roadmap)
8 Appendix

8.1 DATA CONFIDENTIALITY OBLIGATION – FORM LETTER

<table>
<thead>
<tr>
<th>EXPLANATION OF OBLIGATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last name:</td>
</tr>
<tr>
<td>First name:</td>
</tr>
<tr>
<td>Personnel number:</td>
</tr>
<tr>
<td>Department:</td>
</tr>
</tbody>
</table>

Dear Madam or Sir,

Because of the tasks you perform in our organization, data privacy regulations, as described in §5 of the (German) Federal Law for Data Protection (BDSG), apply to you and your work. This law states that you may not collect, process or use personal data.

As stated in §5 of the BDSG you are obligated to maintain data confidentiality. This obligation extends beyond your employment in this organization and applies without exception to all duties related to the handling of personnel matters, organizational secrets, confidential business documents and any other duties described in the work contract.

It is our duty to notify you that violations of data confidentiality are punishable (as described in §§ 43 and 44 of the BDSG, as well as in other relevant legislation), with fines or imprisonment. Copies of the regulations mentioned here (§§ 5, 43, and 44 of the BDSG) are attached.

After signing this document, please return it to your superior who will forward it to the personnel department to be stored in your personnel file. You should keep a copy for your own records.

Place, Date

Signature of superior/ Area representative

I have been informed of the regulations in the Federal Law for Data Protection which apply to my responsibilities in this organization. I understand the consequences of violating these regulations. I accept my obligation to maintain confidentiality as described in §5 of the BDSG.

Employee signature:

Date signed:
§ 5 DATA CONFIDENTIALITY

“Persons employed in data processing shall not collect, process or use personal data without authorisation. On taking up their duties such persons, in so far as they work for private bodies, shall be required to maintain data confidentiality. This obligation shall continue to be valid after termination of their activity.”

§ 43 ADMINISTRATIVE OFFENCES

(2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence,…

1. collects or processes personal data which are not generally accessible without authorisation.

2. holds personal data which are not generally accessible ready for retrieval by means of an automated procedure without authorisation.

3. retrieves personal data which are not generally accessible or obtains such data for themselves or another from automated processing operations without authorisation.

4. obtains by means of incorrect information the transfer of personal data which are not generally accessible.

5. in violation of the first sentence of Section 16 (4) and the first sentence of Sections 28 (5) of this Act, also in conjunction with Section 29 (4) the first sentence of Section 39 (1) or Sections 40 (1) of this Act, uses data for other purposes by transmitting them to third parties, or

6. in violation of the second sentence of Section 30 (1) of this Act, combines the characteristics mentioned in the first sentence of Section 30 (1) with the information or, in violation of the third sentence of Section 40 (2), combines the characteristics mentioned in the second sentence of Section 40 (2) with the information.

(3) administrative offences shall be punishable by a fine of up to 250,000 Euros in case of sub-section 1 above, and by a fine of up to 250,000 Euros in the cases under subsection 2 above.

§ 44 CRIMINAL OFFENCES

(1) Anyone wilfully committing an offence specified in Section 43 (2) of this Act in exchange for payment or with the intention of enriching himself or another person or of harming another person shall be liable to imprisonment for up to two years or to a fine.

(2) Such offences shall be prosecuted only if a complaint is filed. Complaints may be filed by the data subject, the Federal Commissioner for Data Protection and Freedom of Information and the supervisory authority.
8 Appendix

8.3 HANDLING PERSONAL DATA – RECOMMENDATIONS FOR EMPLOYEES

The following recommendations are for employees who work with personal data, including data not available to the public such as work telephone numbers or work locations.

> Do not include personal data in documents if it is not required to complete an assigned task.

> Do not allow any unauthorized person to see your documents or work (for example, Rolodex, print-outs, transcriptions, etc.).

> Do not send out inter-office documents containing personal data without closed and sealed envelopes or other containers.

> Do not send e-mail containing personal data unless it is encrypted.

> Ensure that data medium are safely locked.

> Ensure that personal data in documents and data medium is (legally) removed or destroyed when no longer needed.

> When working at PC or terminals do not leave the workstation without properly ending the session or activating password protection (for example, with appropriate screen savers).

> If your PC can be accessed by other people, ensure that access to personal data is not possible.

> Ensure that personal data cannot be accessed or changed from work places through remote access (home offices, hotels, airports) using data processing and communications devices (Notebooks, Palmtops).

> Give out written or verbal (spoken) information only to clearly authorized persons within the organization.

> Do not provide by telephone, or by other verbal means, personal information about individuals to anyone outside the organization, unless there are specific instructions to do so.

> Written reports containing personal information provided to third parties must be part of official documents with appropriate signatures. If the data concerns internal employees, the responsible personnel department must be notified.

> For all personal information requests which are outside the normal routine requests, or which may violate the regulation of the BDSG, consult a superior or the Data Protection Officer in your organization. The will determine if the information requests can be legally provided.

> If you learn of violations of data protection regulations within your organization, notify your superior or the Data Protection Officer.
8.4 SOFTWARE APPLICATION REGISTRATION FORM – (PROCESSING PERSONAL DATA)

SOFTWARE APPLICATION DESCRIPTION

THE DATA PROTECTION OFFICER

(    ) NEW ENTRY  (Fill all fields below)
(    ) DELETION  (Fill fields 1 and 2)
(    ) MODIFICATION  (Fill fields 1, 2 and all applicable fields)

Place an “x” before applicable items

1. Person/position responsible
   (the department responsible for the content of the mechanized procedures)

   Department:

   Contact person in department:

   Telephone:

2. Procedure name (file name)

3. Specific function of the procedure

4. Authorized user group

5. Data subject groups
   (    ) Employee  (    ) Hourly worker
   (    ) Customer  (    ) Manager
   (    ) Vendor  (    ) Applicant
   (    ) Other  (    ) Trainee
   (    ) Student intern
   (    ) Pensioner
   (    ) Next of kin

   (for employees and former employees, please specify a group)
   (if „Other“ is checked, please enter details here)

6. Procedure content (file structure)
   (attach list of data fields)
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Data medium/volume</td>
</tr>
<tr>
<td>8.</td>
<td>Data processing facilities (Type/Location)</td>
</tr>
<tr>
<td>9.</td>
<td>Back-up strategy</td>
</tr>
<tr>
<td>10a.</td>
<td>( ) internal use of the data</td>
</tr>
<tr>
<td>10b.</td>
<td>Transfer of data to third parties (Identification of data recipient)</td>
</tr>
<tr>
<td></td>
<td>( ) Transfer from data storage</td>
</tr>
<tr>
<td></td>
<td>( ) Automated call procedures</td>
</tr>
<tr>
<td>Data transferred (content description) (If different from No. 6, attach list here)</td>
<td></td>
</tr>
<tr>
<td>10a.</td>
<td>( ) Processed by service provider/contractor (Identification of the contractor)</td>
</tr>
<tr>
<td>11.</td>
<td>Permissibility of data processing and use</td>
</tr>
<tr>
<td></td>
<td>( ) Legal regulations</td>
</tr>
<tr>
<td></td>
<td>( ) Contract or mutual agreement</td>
</tr>
<tr>
<td></td>
<td>( ) Protection of justified interests</td>
</tr>
<tr>
<td></td>
<td>( ) Consent of the data subject</td>
</tr>
<tr>
<td></td>
<td>( ) Other reasons</td>
</tr>
<tr>
<td>12.</td>
<td>Data source</td>
</tr>
<tr>
<td>13.</td>
<td>Date of required deletion of personal data</td>
</tr>
<tr>
<td>14.</td>
<td>How was the data subject informed of the data storage?</td>
</tr>
<tr>
<td>15.</td>
<td>Was the data processing procedure reported to the personnel department (in case agreement with the works committee is required)?</td>
</tr>
</tbody>
</table>
Attachments for these items:
( ) for item 6  File structure (fields)
( ) for item 9  PC security verification
( ) for item 10a Internal data recipient
( ) for item 10b External data recipient
( ) for item 10c Contractee/controller
( ) for item 13  Deletion deadline

Place and date

Signature of department manager
NOTES AND DEFINITIONS FOR THE QUESTIONS

1. General comments
The registration of automated procedures (computerized data sets) with which personal data are stored, for the initial acquisition, as well as for later updates, is a component of the data security law (BDSG). This step enables the Data Protection Officer to fulfil his obligations listed in Section 4g of the BDSG. This form assists the Data Protection Officer in providing to the central registry the correct information concerning automated data processing procedures.

When necessary, department specialists should be contacted to fill in missing information. The registration of non-automated file systems (card indexes) was discontinued in May 2001.

2. Subject of the registration
The registration applies to all personal data of natural persons which can be processed by an automated system. In this case, the application (automated procedure or software program) is registered, not the physical file/database.

3. Terminology (from Section 3 of the BDSG)
“Collection” means the acquisition of data on the data subject.

“Processing” is the storage, modification, transfer, blocking and erasure of personal data.

“Transfer” is the disclosure to a third party of personal data stored or obtained by means of data processing either…
a) through transmission of the data to the third party or..
b) through the third party inspecting or retrieving data held ready for inspection or retrieval.

“Use” is any utilisation of personal data other than processing.

“Controller” is any person or body collecting, processing or using personal data on his or ist own behalf or commissioning others to do the same.

“Third party” means any person or body other than the controller. This shall not include the data subject or persons and bodies commissioned to collect, process or use personal data…

4. Updates to the registration
Additional (new) data sets are to be registered using this Entry Form and its attachments. Changes to, and deletions of, data sets do not require this Entry Form and can simply be reported to the Data Protection Officer.
5. Supplemental references for the items in the Entry Form

For 1) The controller is the department which is responsible for the automated procedure. For procedures which lie in the responsibility of several departments the responsibility for data protection must be determined by the Data Protection Officer case by case.

To be included in the registry the specification of the organizational user number (OU number) is absolutely necessary.

For 2) Name of the procedure (if necessary, the data set)

For 3) List of the fields for which the procedure is used.

For 4) Groups are to be identified, such as personnel clerks, customer service employees, etc.

For 5) In this field the affected groups, for example, employees, former employees, customers, vendors, stockholders, etc., should be listed.

For employees and former employees the appropriate groups should also be checked.

For 6) Here a list of the stored data fields, along with non-standard abbreviations, should be attached.

If the standard format descriptions for data processing files taken from system documentation are attached, it must be ensured that the names or abbreviations for data elements/groups can be easily identified. If not, additional explanations must be attached.

For 7) Storage medium can be: Magnetic tape, magnetic disk, floppy disk, back-up files, microfilm, COM-Fiches, magnetic accounts, punched cards, and so forth.

For 8) For automated data processing the type and location of the DP system in use must be specified (for example Notes Server, host, name of building, in the IT department, in Scale On). Personal computers and/or work processing systems (individual data processing) are considered part of the DP system.

For 9) Specification of the data security measures (data backup, system security, data access protection...).

Where data is stored on PCs or work stations, the requirements listed in Section 9 and the Appendix to Section 9 in the BDSG (Verification of appropriate data protection measures for PCs and work stations) should be followed when completing this item of the form.

For 10) The various types of data used are defined here:

a) interne use (data used exclusively within the company)
Identify the direct recipient of the data (if not included in item 4) and the data medium used.

b) data transferred to third parties
It should be specified whether the data is physically transferred to the third party or is made available on-line to the third party

The data recipients (also associated organizations) are to be identified, as well as the transferred data and the reason for the data transfer

c) data processed by service providers (contractors)

Identification of the contractor

The data exchange between customer/controller and contractor is not classified as a data transfer as long as the data continues to belong to the customer/controller

A single procedure can be used to process several different data sets. If there is not sufficient space in this form to list all datasets, put the list in an attachment to this form.

for 11) The permissibility of data processing (saving, transferring, updating) is linked to various conditions referred to in Sections 4 and 28 of the BDSG.

Where regulations of the Federal Government refer to specific cases of personal data stored in electronic files, these regulations take precedence over the BDSG. Examples of this are rules which apply to financial reporting (HGB, AO) or the transfer of data to social insurance agencies (DÜVO).

Contractual relationships, such as employment contracts or bills of sale, can be classified as quasi-contractual mutual-trust agreements (job applications, for example).

By “justified interests” is meant the own interests of the controller where it concerns the storage of the data. In cases where data is transferred to third parties, “justified interests” refers not only to the own interests of the controller, but also the legitimate interests of the third party and/or the general public. The “justified interests” are only valid, however, if they do not take precedence over the interests of the data subject.

Other reasons are, according to Section 28 of the BDSG, if the data comes from generally accessible sources or the responsible place has permission to publish the data.

The valid admissibility requirements for each case are to be explained in the questionnaire.

for 12) The term “data source” here is understood to mean the logical origin of the data, for example questionnaires, hiring documentation, data from third parties, etc.

for 13) For stored personal data the deletion date (or maximum storage time) it is to be specified.

for 14) According to the BDSG the data subject is to be informed about the first storage of his data whether the data was collected verbally, through forms or personal data collection. As a rule, when personal data is maintained within the framework of the employer-employee relationship in a corporate area it is not necessary to inform the data subject more than once.
6. Supplementary information software procedure questionnaire attachments.

In case where the space provided in the procedure questionnaire for answers is not sufficient, supplemental attachments should be used. There are two types of attachment:

a) Attachment for the questions 6, 10a, 10b, and 10c

When alternate sources of information already exist containing the information requested in the software procedure questionnaire, these may be attached (field descriptions of a data file, for example).

b) Verification of data security measures for PC and word processing systems (attachment for question 9)

Where PC and/or word processing systems exist, this attachment is required.

Januar 2007
8 Appendix

THE DATA PROTECTION OFFICER

QUESTIONNAIRE – PERSONAL DATA STORED IN ELECTRONIC FILES
Attachment for software application description
Question 6, 10 (a-c), 13

Responsible person/position:

OU Number:

File Name:

Attachment for question no. ( )
THE DATA PROTECTION OFFICER

QUESTIONNAIRE – PERSONAL DATA STORED IN ELECTRONIC FILES
Attachment for software application description
(Question 9)

Comment: For PC- and word processing systems with which personal data are processed, data security
measures are stipulated by law. Where data is stored locally on a PC or Laptop, this software application
description should be attached. Responsible person/position

1. Description
The registration of automated procedures (computerized data sets) with which personal data are stored, for the initial acquisition, as well a

1.1 Location of the data processing equipment:

Department/Site:

Plant/Building:

Contact person:

INVENTORY NO:

1.2 Hardware:

Software:

1.3 Operational type:

Offline-operation: yes / no
Online-operation: yes / no

Site host computer:

Network operation: yes / no

1.4 Number of authorized users:
## 2. Security measures

(check applicable)

<table>
<thead>
<tr>
<th>Security measure</th>
<th>Yes</th>
<th>No</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.1 Physical access control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access with identification check</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td>Enclosed area</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td><strong>2.2 System access control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization concept</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td>Password protection</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td><strong>2.3 Data access control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td><strong>2.4 Data transfer control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of available data media</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td>Locked data media</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td><strong>2.5 Data entry control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging/Authorization concept</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td>Security software (such as RACF)</td>
<td>( )</td>
<td>( )</td>
<td></td>
</tr>
<tr>
<td><strong>2.6 Additional security measures:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(add short description)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Place/Date

Department/Manager

Application user
### 8.5 Role of the Data Protection Officer in the ASAP Procedures Model

#### Phase 1: Project Preparation

<table>
<thead>
<tr>
<th>1.1</th>
<th>Project Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>Formulate data protection goals within the context of the Security Policy mission statement of the project.</td>
</tr>
</tbody>
</table>

These principles should be specific and written in easily understood language. Check whether reference should be made to appropriate data protection policies.

| 1.1.1.4 | Specify project success standards (including data protection success standards, such as documents and security level). |

Purpose …. Reach goal values for participation and support Security level and data protection

| 1.1.4.2 | Assign project roles (in particular the roles of the data protection officer for operations, auditing and employee representative) |

I: Purpose …
Change Team member
Auditing
Data protection
Employee representative

II: Describe the project roles …
Auditor
Person responsible for data protection
Employee representative

| 1.1.5.1 | Create work plan |
| 1.1.6.2 | Revise training plan |
| 1.1.6.3 | Register team for training |

### 1.2 Project Flow

| 1.2.1.1 | Determine project communication plan |

| 1.2.1.9 | Agree on standards for quality assurance (also in agreement with the Data Protection Officer) |

Purpose …
… can also happen during implementation process. If necessary, the actual standards can be co-ordinated with auditing and the DPO.
### PHASE 1: PROJECT PREPARATION

<table>
<thead>
<tr>
<th>1.2.2.9 Determine ABAP development standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarify whether departments will be developing their own software and whether ABAP Query is to be used. Create, if necessary, the data protection legal requirements (agreement with the employee representatives, creation of additionally required data protection regulations, employee training, decrease of user-defined programs).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.2.2.10 Establish quality assurance standards for work conditions/ergonomics related to data protection</th>
</tr>
</thead>
</table>
| Purpose …  
The purpose of the task is to establish standards for work organizations, ergonomics and data protection. |
| Procedure:  
1. Determine to what extent the standards for work organizations, ergonomics and data protection are necessary for the implementation. Decide who is responsibility for these tasks (development, departments).  
2. Provide a schedule for these tasks, if needed. Consult the specialists for these areas within the organization (for example, industrial safety, employee representatives, data protection) before finalizing the schedule. |
| Result:  
The decision concerning standards for development is made. |
| Roles:  
Project leader, Change Team Leader, employee representative, Data Protection Officer |

<table>
<thead>
<tr>
<th>1.2.3.1 Determine required systems (Which systems will contain production data?)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>1.2.3.2 Determine client strategy (Which clients will contain production data?)</th>
</tr>
</thead>
</table>

### 1.3 Project Kickoff

<table>
<thead>
<tr>
<th>1.3.1.2 Hold Kickoff meeting (include Data Protection Officer and the employee representative)</th>
</tr>
</thead>
</table>
| Participants:  
Management representative, members of the project team, consultants and additional employees such as the employee representatives and data protection officer |

<table>
<thead>
<tr>
<th>1.1.6.3 Register team for training</th>
</tr>
</thead>
</table>
### PHASE 1: PROJECT PREPARATION

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4</td>
<td>Planning of technical requirements</td>
</tr>
<tr>
<td>1.5</td>
<td>Quality testing project preparation</td>
</tr>
</tbody>
</table>

Review project preparation phase (including part-time participants in the project)

Steps:
1. …
2. Conduct a formal review and get sign-off. Include individuals who are not full-time project members (such as employee representative and the Data Protection Officer).

### PHASE 2: BUSINESS BLUEPRINT

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Project Management Business Blueprint</td>
</tr>
<tr>
<td>2.2</td>
<td>Organizational Change Management</td>
</tr>
</tbody>
</table>

2.2.1 Describe recognized effects on the organization

Add: Assess probability of success and risks from the employees point of view.

2.2.2 Complete the risk assessment by organization leadership.

Purpose …
… to revise assessment elements (for example, for data protection or the involvement of the employee representative) as well as particularly critical elements of the comprehensive restructuring program

2.2.2.4 Conduct risk workshops for the organization leadership

Purpose…
… those who are responsible for the design and review of action plans (such as auditors and the Data Protection Officer) are required to participate in the Risk Assessment Workshops for managers.

2.2.2.4a Conduct Risk Assessment Workshop for Employee Representatives, Data Protection Officer/ Auditor and, if necessary, representatives of the organizational leadership

(Employee representatives involved in the project may participate in this workshop or a separate workshop held only for this group)
### 8 Appendix

#### PHASE 2: BUSINESS BLUEPRINT

<table>
<thead>
<tr>
<th>2.2.3 Develop mentor strategy</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>2.2.4.4a Conduct risk workshop for Data Protection Officer/Auditor and financial auditors</th>
</tr>
</thead>
</table>

**Purpose…**

Purpose of this task is it to present risk avoidance strategies and plans of action - as well as the appropriate responsibilities - in order to minimize the implementation risks, particularly in view of data protection and the KonTraG ("Gesetz zur Kontrolle und Transparenz im Unternehmensbereich", in English "Corporate Sector Supervision and Transparency Act").

**Procedure (see 4.2.2.4):**

**Result**

Quantification of the implementation risks and definition of the intended actions and task distribution for the prevention of these risks.

<table>
<thead>
<tr>
<th>2.2.5.3a Develop tools for risk assessment pertaining to data protection</th>
</tr>
</thead>
</table>

**Purpose…**

To assess the possible effects of these risks on the implementation of the SAP system. The evaluation should also take into account the intended changes in the organization and the flows of information.

<table>
<thead>
<tr>
<th>2.2.6.3a Integrate results of the risk assessment pertaining to data protection</th>
</tr>
</thead>
</table>

The results are to be addressed. The issue of how data protection will be assured should also be considered at this point.

<table>
<thead>
<tr>
<th>2.2.8.2 Establish and implement procedures for knowledge transfer</th>
</tr>
</thead>
</table>

**Purpose…**

…the transfer of knowledge. This may require both coordination with, and involvement of, the persons responsible for data protection.

<table>
<thead>
<tr>
<th>2.3 Project Team Training</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>2.3.1.1 Revise Training Plan</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>2.3.1.2 Prepare Training</th>
</tr>
</thead>
</table>
## PHASE 2: BUSINESS BLUEPRINT

<table>
<thead>
<tr>
<th>2.4</th>
<th>Development system environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.1</td>
<td>Design technical concept</td>
</tr>
</tbody>
</table>

#### 2.4.1.5 Define change request management

The results are to be co-ordinated - both for normal operation and for emergency plans - with internal auditing and the persons responsible for data protection.

#### 2.4.1.8 Reconcile the technical concept with information from the auditors and the Data Protection Officer

Purpose...

..that the steering committee receives appropriate information from auditing and the DPO… which correspond to the requirements of this implementation and the legal regulations concerning data protection.

#### 2.4.2.5 Create user master record for project team and review the definition specification of authorizations for Customizing tables

#### 2.4.4.1 Conduct Basis System Administration Workshop

#### 2.4.4.5 Check system administration functions and turn on table logging

<table>
<thead>
<tr>
<th>2.5</th>
<th>Organizational structure</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>2.6</th>
<th>Business process definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6.1.1</td>
<td>Plan business processes workshops</td>
</tr>
</tbody>
</table>

#### 2.6.3.1 Specify requirements for business processes

Propose possible outcomes for qualification planning and data protection organization to be discussed.

To establish requirements for the SAP reference model, taking into consideration the options available for the qualification and data protection organization.
## PHASE 2: BUSINESS BLUEPRINT

| 2.6.3.4 | Determine necessary interfaces and, because of the transmission of personal data, get agreement with the Data Protection Officer where appropriate. |
| Purpose... |
| To get agreement, where necessary, with the employee representative and the Data Protection Officer on the data protection concept. |

| 2.6.4.2 | Optimize business process definitions and models with involvement of employee representation. |

| 2.6.7 | Create plan for user training and documentation |
| Procedure: |
| ...should be documented. Here data protection regulations should be addressed with involvement of the Data Protection Officer. |

### 2.7 Quality Check Business Blueprint

| 2.7.1.2a | Sign-off for Business Blueprint phase from employee representation and data protection officer. |
| Purpose of this task is to obtain sign-offs from project management and other project participants, i.e. internal audit, Data Protection Officer and employee representation. |
| Roles: Project manager, steering committee, auditing, data protection, employee representation |
| 2.7.1.3 Confirm that checklist 1 is complete |

## PHASE 3: REALIZATION

| 3.1 | Projektmanagement Realisierung |
| 3.1.6.2 | Update Project Management Plan |

| 3.2 | Organizational Change Management discussions |
| 3.2.2.5 | Carry out meetings concerning risk management with key groups (i.e. auditing, employee representation and data protection) |
| Flow: |
| 2... the steering committee, auditing, employee representation, the Data Protection Officer and, if necessary... |
## PHASE 3: REALIZATION

<table>
<thead>
<tr>
<th>3.3</th>
<th>Training of the project team, realization</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4</td>
<td>Baseline configuration and sign-off</td>
</tr>
<tr>
<td></td>
<td>3.4.4.3 Prepare meeting for the baseline/sign-off</td>
</tr>
<tr>
<td></td>
<td>Invite groups which are not part of the core project team (auditing, data protection and employee representation).</td>
</tr>
<tr>
<td>3.5</td>
<td>System management</td>
</tr>
<tr>
<td></td>
<td>3.5.3.2 Check daily test procedures</td>
</tr>
<tr>
<td></td>
<td>In addition, confirm that security violations are checked regularly.</td>
</tr>
<tr>
<td></td>
<td>3.5.3.3 Check transport procedures</td>
</tr>
<tr>
<td></td>
<td>Purpose...</td>
</tr>
<tr>
<td></td>
<td>... establish procedures for quality assurance, where appropriate with the involvement of auditors and persons responsible for data protection.</td>
</tr>
<tr>
<td></td>
<td>3.5.6.1 Define security concept of the production system</td>
</tr>
<tr>
<td></td>
<td>Procedure:</td>
</tr>
<tr>
<td></td>
<td>[4] Coordinate the results, where appropriate with auditing, employee representation and the persons responsible for data protection.</td>
</tr>
<tr>
<td></td>
<td>3.5.6.6 Create R/3 System Operator’s Guide</td>
</tr>
<tr>
<td></td>
<td>Procedure: Process flow</td>
</tr>
<tr>
<td></td>
<td>[1]... together, add references to data protection where needed.</td>
</tr>
<tr>
<td>3.6</td>
<td>Detail configuration and sign-off</td>
</tr>
<tr>
<td></td>
<td>Prepare meeting for detail sign-off</td>
</tr>
<tr>
<td></td>
<td>Procedure:</td>
</tr>
<tr>
<td></td>
<td>Process flow</td>
</tr>
<tr>
<td></td>
<td>[3] Distribute the handouts which describe the possible scenarios to the participants. Include here the quality assurance in the production system – including auditing and data protection viewpoints. The participants...</td>
</tr>
</tbody>
</table>
### PHASE 3: REALIZATION

| Prepare Quality Assurance (QA) in the Production System with respect to data protection and auditing |
| 3.6.5.2 Review and sign-off on detail configuration |
| Purpose... the properly working configuration and data protection provisions are enough. |
| Process flow: 3A Summarize the results and describe improvement work that may be needed. |

#### 3.7 Prepare and coordinate ABAP development

Purpose of this work package is to prepare and coordinate the ABAP- and ABAP/4 query development. Confirm that employee representation and persons responsible for data protection are involved in the development of ABAPs and department programs that will process personal data.

##### 3.7.1.1 Establish and register user-ids for development

Check whether all planned developers (including external developers) are obligated to comply with data protection rules. Make sure that developers are under obligation to maintain confidentiality of personal data before work is started.

##### 3.7.2.1 Define business application hierarchy, development classes and authorization groups

#### 3.8 Development of data transfer programs

#### 3.9 Development of interface programs for applications

##### 3.9.1.1 Complete the detailed definition of the interfaces

Purpose...
Some of the key items that you must consider are...
... data protection legal regulations, rights of the employee representation
4. Determine the data to be exchanged
... in the interface Advisor). Confirm compliance with current regulations for data protection.

#### 3.10 Development of data transfer programs

##### 3.10.1.2 Check the approval

Ensure the agreement of employee representatives and inclusion of the Data Protection Officer during the creation of personal data related ABAPs and InfoSets for Queries.
### PHASE 3: REALIZATION

#### 3.11 Development of Reports

<table>
<thead>
<tr>
<th>3.11.1.2</th>
<th>Check “limited usage” and legal regulations; obtain, where necessary, approval of the employee representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>..... is developed. Pay attention to the inclusion of the Data Protection Officer and where appropriate the employee representation for reports with personal information. A report...</td>
</tr>
</tbody>
</table>

**Process flow:**

2A In the area of requests for reports containing personal data, it must be ensured that regulations concerning data protection (legal basis/limited usage), co-determination rights of the employee representative, and business necessity are followed.

<table>
<thead>
<tr>
<th>3.11.2.2</th>
<th>Test and evaluate reports and their authorization checks</th>
</tr>
</thead>
</table>

#### 3.12 Development of forms

<table>
<thead>
<tr>
<th>3.12.1.2</th>
<th>Check approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process flow:</td>
<td>1. Check the defined forms and modify them as necessary to comply with data protection guidelines.</td>
</tr>
<tr>
<td></td>
<td>... is created.</td>
</tr>
</tbody>
</table>

#### 3.13 Processing of the authorization concept

**Process flow:**

1. Ask questions:
   > Which Security Level is necessary for your data?
   > Which data protection legal requests exist?

3. Make your security implementation concept known... to check effects on data owners.

Explain the implementation framework and, where appropriate, the data protection regulations. Then consult ...

<table>
<thead>
<tr>
<th>3.13.1</th>
<th>Prepare detailed definition of the authorization concept – Formulate data protection requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.13.1.1</td>
<td>Develop details of the authorization strategy for the enterprise</td>
</tr>
<tr>
<td></td>
<td>Define general roles for the auditor, the external auditors, data protection responsible persons and the representatives for the employees.</td>
</tr>
</tbody>
</table>
### 3.13.1.3 Discuss authorizations with data owners, when substantial changes are made, e.g. with personal data (opposite 2.6.3.4) inform the relevant authorities (e.g. commissioner for data protection).

**Purpose**

...notify the user. Examine the personal data, when necessary with help from the responsible persons (such as the data protection officer) to determine if the regulations are upheld.

### 3.13.2.1a Determine available authorization groups – ABAPs and tables with respect to data protection

### 3.13.3.5 Sign-off on authorization concept

**Purpose**

... to get sign-off from the responsible data owner, auditing, and if needed the data protection officer and employee representative.

**Tip:**

... involve the enterprise auditors, such as internal auditors and data protection officers.

### 3.14 Set up archiving procedures

### 3.14.1.1 Establish the archiving strategy (include the data protection deletion deadline regulations)

**Purpose**

... will be reduced. Both the data protection legal retention and deletion timeframes must be considered.

### 3.15 Final integration test

### 3.16 Documentation and training materials for users

### 3.16.1.1 Define, and modify as necessary, documentation requirements for users (see 2.6.7 – Create plan for user training and documentation)

### 3.16.2.2 – Create user documentation

**Purpose**

... in the SAP system.

The inclusion of references to the adherence to the data protection regulations (e.g. for business processes with personal data) in this documentation is to be reviewed.

### 3.17 Quality test, realization

- Test of process flows and screens based on prototypes
- Evaluation of software ease-of-use
### PHASE 4: PRODUCTION PREPARATION

<table>
<thead>
<tr>
<th>4.1</th>
<th>Project management and production preparation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>User training</td>
</tr>
<tr>
<td></td>
<td>4.2.2.1 Carry out user training</td>
</tr>
<tr>
<td></td>
<td>Purpose ...</td>
</tr>
<tr>
<td></td>
<td>... complete. This should include references</td>
</tr>
<tr>
<td></td>
<td>to the relevant current enterprise policies</td>
</tr>
<tr>
<td></td>
<td>concerning protection of information and the</td>
</tr>
<tr>
<td></td>
<td>relevant legal decisions.</td>
</tr>
<tr>
<td>4.3</td>
<td>System management</td>
</tr>
<tr>
<td></td>
<td>4.3.0 Carry out Basis and system administration workshop (related to data protections and auditing requirements – was previously 2.4.4.1)</td>
</tr>
<tr>
<td></td>
<td>4.3.1.3 – Train personnel for system administration – include data protection and audit requirements</td>
</tr>
<tr>
<td></td>
<td>Purpose ...</td>
</tr>
<tr>
<td></td>
<td>... include user administration, auditability,</td>
</tr>
<tr>
<td></td>
<td>data protection as well as escalation procedures.</td>
</tr>
<tr>
<td>4.4</td>
<td>Detailed planning for cutover and support</td>
</tr>
<tr>
<td></td>
<td>4.4.2.1 Define Help Desk procedures with</td>
</tr>
<tr>
<td></td>
<td>respect to data protection regulations</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
</tr>
<tr>
<td></td>
<td>1. ...</td>
</tr>
<tr>
<td></td>
<td>... about organization and processes, especially the enterprise policies in effect and legal concepts for data protection.</td>
</tr>
<tr>
<td>4.5</td>
<td>Cutover</td>
</tr>
<tr>
<td>4.6</td>
<td>Quality test and production preparations</td>
</tr>
<tr>
<td></td>
<td>... The final check of all technical</td>
</tr>
<tr>
<td></td>
<td>preparations, including the appropriate data</td>
</tr>
<tr>
<td></td>
<td>protection measures, is absolutely necessary.</td>
</tr>
</tbody>
</table>

### PHASE 5: GO-LIVE AND SUPPORT

| 5.1 | Production support                           |
|     | 5.1.2.2 Resolve issues and problems related to data protection regulations and policies |
| 5.2 | End of project                              |
8 Appendix

8.6 CHECKLIST OF AUDITABILITY REQUIREMENTS

8.6.1 REQUIREMENTS FOR AUDITABILITY

8.6.1.0 IS THE JAVA STACK ACTIVE?

Check the instance parameter rdisp/j2ee_start using the RSPARAM and/or RSPFPAR reports or with the RZ10 and/or TU02 transactions:

Value = 0: The JAVA stack is not active and requires no further attention.

Value = 1: The JAVA stack is active and the JAVA engine can be started and used by appropriate programs. In this case further checks are necessary in order to guarantee required data protection and security levels for the Netweaver JAVA stack. (These checks are not included in this check list or the data protection manual for SAP ERP 6.0 30.5.2008.)

Use TU02 to review the history of the JAVA stack activation settings.

8.6.1.1 HARDWARE

For each case below, is there up-to-date documentation describing…

> On which computers (application servers/work stations/terminal, etc.) SAP relevant data processing (including data delivered by SAP systems and/or data made available to SAP systems, e.g. time recording systems) takes place?

> On which computers SAP development, quality assurance and productive systems run? Does this information agree with SYSTEM→STATUS and the TSYST table (view with SM31 or SE16)? / T000 and T001

> Which operating systems are installed on these computers? Compare the various systems using SYSTEM→STATUS.

> Which computer systems are used (whether Windows, UNIX, or IBS iSeries computers are used as the server, which client computers are in use)?

> Which network components (for example, routers) are used?

> Who is responsible for monitoring and maintaining computer operations?

> Which Service Level Agreements (SLA) are in place? Which agreements related to Data Protection are included?

Is an up-to-date network overview available in graphical and/or written form?

Is a corresponding up-to-date configuration overview and/or network description available?
## 8.6.1.2 OPERATING SYSTEM AND LOW-LEVEL SOFTWARE

Is there written documentation describing…

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; Which operating systems (including version number) are used? Compare with &quot;ys&quot; in the OK-Code or SYSTEM STATUS in the different systems</td>
<td></td>
</tr>
<tr>
<td>&gt; Which database systems or data management systems (and release) are used? Check SYSTEM STATUS in the different systems.</td>
<td></td>
</tr>
<tr>
<td>&gt; Which network operating system is run?</td>
<td></td>
</tr>
<tr>
<td>&gt; Which network services are active in the server domain and which are deactivated?</td>
<td></td>
</tr>
<tr>
<td>&gt; Which routers and firewall systems separate the SAP server domain and the SAP network from other networks (in particular external networks)?</td>
<td></td>
</tr>
<tr>
<td>&gt; Is network encryption used? If so, on which routes?</td>
<td></td>
</tr>
<tr>
<td>&gt; Between application servers</td>
<td></td>
</tr>
<tr>
<td>&gt; Between application servers and clients</td>
<td></td>
</tr>
<tr>
<td>&gt; Between application servers and printers</td>
<td></td>
</tr>
<tr>
<td>&gt; Which maintenance accesses are provided, in particular for remote maintenance (hardware or software maintenance)?</td>
<td></td>
</tr>
<tr>
<td>&gt; Will SAP encryption techniques be implemented (NSC/SSF)? (SNC=Secure Network Communication, SSD=Secure Store &amp; Forward)</td>
<td></td>
</tr>
<tr>
<td>&gt; Will digital signatures be used?</td>
<td></td>
</tr>
</tbody>
</table>

Which access rights are set up (and for whom) for the SAP ERP database?

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a user and authorization concept for SAP objects which applies to the access rights granted on the operating system and network levels of the SAP database server?</td>
<td></td>
</tr>
<tr>
<td>Is it possible for anyone, other than system administrators, to access SAP ERP tables and database at the operating system level?</td>
<td></td>
</tr>
<tr>
<td>Is a database query language available for the SAP ERP database? If yes, can the query language pose a threat to the integrity and auditability of the SAP system?</td>
<td></td>
</tr>
<tr>
<td>Will this query language be used without restrictions (for example, to make changes to the database)?</td>
<td></td>
</tr>
</tbody>
</table>
### 8.6.1.3 PROGRAMMING TECHNIQUES

**Do obligatory program guidelines exist?**

Has it been specified...

1. Which programming languages external to SAP will be used and whether these programs can access SAP (for example, SQL, JAVA, ...)?

2. Which program generators or other software engineering tools are operational in the SAP system (ABAP Query, Report Writer, etc.)?

**In which systems/clients can software development take place?**

1. Check the system changeability settings

2. Check the client changeability settings in table T000 for the systems in question (including recording obligation).

3. Check the assigned authorizations for the object S_DEVELOP with Activity 01 (create) and 02 (change), as well as object type PROG

4. Check the assigned developer key in the DEVACCESS table for the systems/clients in question.

**In which systems/clients may/can Customizing settings be changed?**

1. Check the client settings in table T000 on the systems in question.

2. Check the assigned authorizations for the object S_TABU_DIS (activity 02) and for S_TABU_CLI ("X").

**Is there a written procedure for making changes in the production systems?**

> Who has which authorizations in the Change and Transporting System (CTS)? Use the Authorization Information System SUIM (users by authorization values) to analyze the assigned authorizations for the authorization object S_TRANSPRT.

**Are there any Customizing tasks and programs that are not adequately documented and described?**

**After release updates or significant changes to the system is the system documentation updated and system auditability maintained?**

> Use the CTS Information System (transaction SE03) to analyze whether the transported customer-defined objects are adequately and clearly documented.

**Is protected personal data transferred from the productive SAP System to a Data Warehouse (SAP Business Warehouse / SAP NetWeaver Business Intelligence) for general evaluation?**
## TESTING PROGRAMS AND CUSTOMIZING SETTINGS

Will special test data be created for the quality assurance system (for example, with tools to make personal data anonymous)?

Will test runs take place using specially created test data or with production data?

- Perform a random check on the data (for example, by calling up the relevant master and transaction data in the appropriate modules and clients, or in the quality assurance client in the consolidation system).

Is it ensured that a test run using real data is only carried out in the following cases:

- With the same authorizations that the testers have in the production system? Use SUIM to analyze the authorizations in the quality assurance / test systems.
- Where rights exceeding those of the testers (programmers, quality assurance team, departments) have been assigned (for example, all rights for the Human Resources director), are tests performed using the dual verification principle?
- With the involvement of the department that is the owner of the data?

Is it ensured that the non-anonymous test material, with the exception of the test data to be documented, is safely destroyed?

Are testing tools (such as SAP internal Computer-Aided Test Tools (CATT)) used, and if yes, by whom?

- Use the authorization information system SUIM to analyze the user master records.

Is the following specified?

- Which data may be used for testing programs and for performing the final test in the systems and clients upstream of the production system? Check the PLANNED specifications (a required test concept) for conformity with the transports to the quality assurance system (test system) and its clients (transaction SE03 or using the AIS report RSWB0040).
- Who provides suitable test data?
- Which “anonymizing” procedures are used?
- Must “anonymized” test data be used?
- Which department is responsible for formulating the programming and change requests?
## 8 Appendix

### TESTING PROGRAMS AND CUSTOMIZING SETTINGS

Are external persons used for testing the program and for program maintenance?

| > Are there any special specifications for security measures to be taken (for example, for protecting the documentation from being overwritten by client copies)? |
| > In particular, check the delivery and transport routes, as well as the assigned authorizations in the clients used for testing. |

### PROGRAM DOCUMENTATION

Is the machine-assisted documentation used for the development of user-defined objects?

| > Use transaction SA38 (GOTO DOCUMENTATION) or SE38 to examine the Z- and Y- reports and use SE11 to examine the table documentation for the Z- and Y- tables. |

Does the documentation describe

| > Which program calls which other programs |
| > Which tables are processed |
| > Which authorization checks are provided |
| > Which input values are allowed |
| > The other components of the object? |

Is it ensured that all program changes and changes to tables controlled by programs are recorded through the (restricted) granting of the authorizations (object S_TRANSPRT) and corresponding settings in systems and clients?

Does a corresponding granted right ensure that the document is protected?

| > Which persons have developer rights (such as S_CTS_DEVELO), who has administrator rights (such as the profile S_CTS_ALL), and who has project manager rights (for example, the profile S_CTS_PROJEC), or comparable rights? Use SUIM (standard authorizations) to check the authorization object S_TRANSPRT. |
| > Or can anyone, if necessary, release and execute all transports using general authorizations (such as SAP_ALL)? |

Are the CTS files adequately protected at the operating system level?

| > Check the access authorizations for the SAP transport files in the directory \usr\sap\trans at the operating system level. |
PROGRAM DOCUMENTATION

Has each program been documented with at least the following elements?

> Application areas of the program

> Structure and description of the program

> Process descriptions (if required)

> A data flow plan

> A description of the check tables or the view structure

> A description of the integration relationships

> Screens, forms used

> A program list (most recent version)

> A log of the final test and a signed exception log

> The test data used

> Instructions for scheduling and post processing work

For this purpose, call up the online documentation (SE38 DISPLAY documentation) and check the program files for the internally developed programs

Is there a manual that contains all the information necessary for using the company-tailored ERP System and that adequately explains the meaning of the required input data?

> Check the user/applications and training manuals.

Have the systems (table TSYST) and clients (table T000), and delivery routes (table TASYS), consolidation routes (table TWSYS), and transport layers (table DEVL) been adequately documented, and do the system settings (for example, the system changeability in T000) ensure that they are maintained?

Are the RFC interfaces adequately documented and protected?

> Which authorizations are assigned for the object S_RFC, and which users have these authorizations?

> Check the corresponding relevant system parameters using report RSPARAM.

System parameter: auth/rfc_authority_check = 1 or 2.
System parameter: snc/accept_insecure_r3int_rfc = NOT 1
System parameter: snc/accept_insecure_rfc = 0

> Use transaction SM58 to analyze the RFC log for undocumented RFC calls.
## Release Procedures

Has an organizational procedure been developed for releasing new or changed functions in order to process protected personal data, and has the release procedure been protected with the appropriate access rights in the CTS? Have the data backup and data protection interests been adequately taken into account? Check whether organizational regulations have been implemented through the appropriate assignment of authorizations for the S_TRANSPRT object.

Is the following documented?

> Who is responsible for releasing the program in line with the Data Protection Act, and, in particular, who is responsible for checking the legal basis, the necessary technical and organizational measures (special authorization checks), and the documentation? Check this against the authorizations assigned for the object S_TRANSPRT.

> Who provides the data for the program run?

Is a release log created?

> Use transaction SE03, report RSWBOSSR to check the texts documenting tasks.

Is the transfer of released objects to the production clients defined?

> Check the assigned authorizations for the object S_TRANSPRT: who can execute appropriate transports?

Is there sufficient documentation of the test routines and sequence of events used for confirming that the procedure has been installed properly and that the program runs correctly?
### APPLICATION DEVELOPMENT

Is the following documented?

> Which persons are responsible for ABAP/query/Ad Hoc Query development?

> Which persons are responsible for SAP procedures release upgrades and maintainence?

> Which parts of the procedure have been developed internally and which have been developed by a software company?

Is adequate documentation provided with regard to the following?

> How long has each SAP procedure been used in production

> When significant changes occurred in the procedure and when new modules, functions, or applications were added

> Who is responsible for requesting procedure changes

> How such changes should be executed in both routine and emergency cases.

Is there a summary and a brief description of the SAP procedures deployed at different times?

> Check the authorizations granted for the S_TRANSPRT object: Who can execute corresponding transports?

Are the test routines and test runs for checking that the procedure has been installed correctly and that the program runs correctly sufficiently documented?

### USER SERVICE/SYSTEM ADMINISTRATION

Is the following defined?

> Who is responsible for computer operations (system administration)?

> Who is responsible for procedures (software administration)?

Use transaction SUIM to check the information against the user authorizations

Have the system administration actions been logged adequately?

Is it stipulated who, and when, will evaluate this log, and for what purposes?

> Check how the logs are used and evaluated.
### USER SERVICE/SYSTEM ADMINISTRATION

<table>
<thead>
<tr>
<th>Question</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have all the procedure changes been automatically and adequately logged</td>
<td>(in the CTS and by means of change logs)?</td>
</tr>
<tr>
<td>&gt; Use SE03 to check the recording obligation, in particular, in the</td>
<td>clients concerned (table T000) as well as whether logging is complete in the CTS</td>
</tr>
<tr>
<td>Have these logs been stored in such a way that they are adequately</td>
<td>protected against manipulation?</td>
</tr>
<tr>
<td>&gt; Check the assigned rights of access to the CTS files. Who can</td>
<td>archive and/or delete the logs at the SAP and operating system levels</td>
</tr>
<tr>
<td>Is the following documented outside the SAP System?</td>
<td>(SCD0 action 06).</td>
</tr>
<tr>
<td>&gt; Which persons manage the authorizations (details on these persons)?</td>
<td></td>
</tr>
<tr>
<td>&gt; Which data the user service has access to, or who can carry out a</td>
<td>trace process (transaction ST01)?</td>
</tr>
<tr>
<td>&gt; Which data is logged for these accesses?</td>
<td></td>
</tr>
<tr>
<td>&gt; Use transaction SUIM to check this information.</td>
<td></td>
</tr>
<tr>
<td>Are malfunctions and measures for eliminating these malfunctions</td>
<td>documented (date, time) in a malfunction log book outside the SAP ERP</td>
</tr>
<tr>
<td>Is the following documented outside the SAP ERP system and in a</td>
<td>system and in a reviewable form?</td>
</tr>
<tr>
<td>Are the steps involved in both user and authorization administration</td>
<td>(configuring, assigning passwords, assigning rights, deleting/changing</td>
</tr>
<tr>
<td>Is there compulsory logging of all changes in the data processing</td>
<td>during transfers to other departments or end of employment) adequately</td>
</tr>
<tr>
<td>Will SAP ERP HCM (Personnel Administration and Organizational</td>
<td>documented and organized to be executed promptly?</td>
</tr>
<tr>
<td>COMPUTER CENTER OPERATIONS</td>
<td></td>
</tr>
<tr>
<td>Is the system console located in a protected area and protected</td>
<td>against misuse?</td>
</tr>
<tr>
<td>Can the calendar date be changed?</td>
<td></td>
</tr>
<tr>
<td>Is there compulsory logging of all changes in the data processing</td>
<td>system programs on which the SAP software runs?</td>
</tr>
<tr>
<td>Is the system administrator’s password for the systems in question</td>
<td>changed regularly and is it kept suitably confidential?</td>
</tr>
<tr>
<td>Is financial accounting…</td>
<td></td>
</tr>
<tr>
<td>&gt; within the SAP ERP system operations?</td>
<td></td>
</tr>
<tr>
<td>&gt; outside the SAP ERP system operations?</td>
<td></td>
</tr>
<tr>
<td>&gt; Is the evaluation procedure regulated? (Reports)</td>
<td></td>
</tr>
</tbody>
</table>
Is there computer center reporting for checking of observed security breaches?

Are these reports regularly evaluated by the auditing department and/or the person responsible for data protection?

Are operator instructions (User Guide) provided for how to respond to system messages?

Are layers logged and are there any regulations governing
> Management?
> Evaluation?
> Storage?

Are there any storage and deletion time periods for computer center documentation (logs, work schedules, etc.)?

Is any documentation available for emergencies?

Are the circumstances for using a stand-by system clarified?

Has the assignment of user authorizations in a stand-by system been specified?

Are there generally two employees present in the computer room per shift?

Are functions restricted in sensitive areas?

8.6.1.4 ADDITIONAL CHECK PROCEDURES
Check also the data backup measures in accordance with Article 9 of the German Federal Data Protection Act in paragraph 3 of the checklists.

8.6.2 CHECK OF SPECIAL REGULATIONS WHICH TAKE PRECEDENCE
(SUCH AS CURRENT COMPANY AGREEMENTS CONCERNING ORGANIZATIONAL AND TECHNICAL MEASURES)

USER AUTHORIZATIONS APPENDIX

Is the appendix kept up to date?

Is the appendix managed manually or partially automated?

If the appendix is generated automatically, perform checks with the appropriate function:
> Use report RSUSR002 to gain an overview of the users and the assigned profiles

> Use report RSUSR002 to evaluate a specific object if you only want to search for users with access to certain authorization objects

> Use report RSUSR003 to check the standard users

> Use reports RSUSR008 and RSUSR009 und RSUSR008_009_NEW to check the users who have critical authorizations.
8 Appendix

USER AUTHORIZATIONS APPENDIX

Depending on the form of the appendix, compare the list with the current status of the tables (by means of SA38 and the corresponding RSUSR* ABAPs).

If necessary, compare the TARGET and ACTUAL status of the appendixes in the form of PC files in the .dbf or .xls format with a corresponding MS Query SQL Query.

Also compare the additional access protection checks under the column ‘Checking Data Protection and Data Backup Measures in Accordance with Article 9 of the German Federal Data Protection Act’.

8.6.3 ADDITIONAL CHECK PROCEDURES

When the technical and organizational measures implemented in accordance with Article 9 of the German Federal Data Protection Act and the appendix to this Act are checked, the appendix numbering system is used, even if this sometimes leads to individual check points being listed twice. Only those points relating to SAP Software are listed. The key points are “Access control”, “Order control”, and “Availability control”. These points deal with areas that must be managed using technical or organizational means outside the SAP System. Where appropriate, suggested checks for these areas are also included.

8.6.3.1 ITEM 1: ACCESS CONTROL (PHYSICAL ACCESS)

According to Item 1, ‘Unauthorized persons must be denied access to data processing systems that process or use personal data (physical access control)’.

This requirement is not relevant to SAP ERP software.

8.6.3.2 ITEM 2: ACCESS CONTROL (SYSTEM ACCESS)

Item 2 of the appendix to Article 9 of the German Federal Data Protection Act stipulates that ‘the use of data processing systems by unauthorized persons must be prevented (operations access control)’.
AUTHENTICATION

Is it ensured that all SAP users have their own user master record?

Perform random checks to establish whether all users in the departments concerned are in the list of authorized users (report RSUSR002).

Use RSUSR002 to perform further checks on the list of users for possible general users, for example, ‘warehouse’ or ‘personnel administrator’, or similar.

> Are there any specifications for secure passwords? Are the illegal passwords adequately maintained in table USR40?

> Which settings are available for the minimum password length? Use RSPARAM to check the parameter login/min_password_lng.

> Which settings affect the creation of new passwords? Use RSPARAM to check the following system parameters:
  Minimum number of digits: login/min_password_digits
  Minimal number of letters: login/min_password_letters
  Minimum number of special characters: login/min_password_specials

> Are users automatically forced to change their password? What is the setting for password change? (recommendation: 60 or 90 days). Use RSPARAM to check the parameter login/password_expiration_time.

> Is the connection terminated after a certain number of failed attempts (3)? Use RSPARAM to check the parameters login/fail_to_session_end and login/fail_to_user_lock.

> Is the automatic creation of the SAP* user deactivated? Use RSPARAM to check the parameter login/no_automatic_user_sapstar (the value should be 1 when the user is deactivated).

> Are inactive users automatically logged off? Use RSPARAM to check the parameter rdisp/gui_auto_logout. (Warning! With the SAP automatic logout, data typed in, but not yet saved before the logout, will be lost. To avoid this problem, use a screen-saver with automatic time-out and password protection.)

> Have the standard users SAP*, DDIC, SACPIC, and EARLYWATCH been adequately protected? Use RSUSR003 to see the status of the user master records (password changes, quality, blocking)

> Use report RSUSR200 to check inactive users with initial passwords
## AUTHENTICATION

Are other methods used, for example, chip cards, for authentication on the frontend computer when the computer is in more or less publicly accessible rooms?

Can the user start the screen-saver to block his screen without logging off?

Is the password protection activated at the PC operating system level, in particular at locations open to the public?

Is the sleep-mode activated after a long period of time? After how many minutes?

> In particular, check the computers that are accessible to the public.

Is special security software used to ensure data security on the PCs?

Is the SAP data encrypted by means of Secure Store & Forward (SSF) or Secure Network Communications (SNC – data privacy protection)? If yes, which data is encrypted?

Is it ensured that protected data cannot flow to unprotected systems from the SAP ERP system via the download function and/or mail?

> Check the authorizations assigned for the object S_GUI.

> Use XXL List Viewer functions to check access to programs.

Is it ensured that access for remote maintenance (in client 066) can only be granted when remote maintenance is explicitly requested?

Are the configured user master records locked at all other times?

Is logging activated (transaction SM19, Security Audit Log) during remote maintenance?

Is the log subsequently evaluated?

Who has authorizations to create RFC connections (SM59) which permit access to data through client 066?
8.6.3.3 ITEM 3: ACCESS CONTROL (DATA ACCESS)

Thirdly, it must be ensured that persons authorized to use a data processing system can only access the data they are authorized to access and that personal data cannot be read, copied, modified, or removed without authorization during processing or use, or after it has been saved (data access control).

**ACCESS PROTECTION**

Are users/functions/rights assigned?

In addition to the overview of users in RSUSR002, is there also a table that identifies the current status of users and authorizations?

Is the user group differentiated in the authorization master record, that is, is it maintained by department or in relation to cost centers? Use RSUSR002 → Display all users → ‘other view’ to analyze the user groups.

Are the comprehensive general authorizations (such as SAP_ALL) restricted to well-protected emergency users (with compulsory logging)?

Are there additional protective measures for these comprehensive general authorizations (for example, through organizational regulations)?

> Use the Authorization Information System (transaction SUIM) to check who has the SAP_ALL profile and who has comparable comprehensive authorizations.

> Check whether compulsory logging in the Security Audit Log is activated for these users in the production environment (transaction SM19).

> Check the logs in the production environment for assignment to comprehensive authorizations (such as SAP_ALL).

Are the sensitive tables adequately protected by table authorizations?

> Analyze the table classes in the table TDDAT for the authorization object S_TABU_DIS. Use transaction SUIM (Users by complex selection criteria) for the authorization object S_TABU_DIS to subsequently check which users have access to these table classes.

Are the sensitive programs adequately protected by report classes?

> Use report RSCSAUTH to analyze the assigned report classes for the reports to be protected.

Alternatively, is end-user access limited to report trees?

> Check whether the use of the transaction SA38 is protected.
<table>
<thead>
<tr>
<th>ACCESS PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are all the transactions that are to be protected either locked (view using report RSAUDITC) or provided with an authorization check for the object S_TC0DE?</td>
</tr>
</tbody>
</table>

> Analyze table TSTCA or use transaction SE93.

<table>
<thead>
<tr>
<th>Is the scope of the authorization check reduced in critical transactions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; Check the parameter auth/no_check_in_some_cases. If the parameter value is Y, use SU24 to determine which checks have been deactivated/changed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is it ensured that the dual verification principle is applied for maintaining and activating authorizations and profiles, as well as for user maintenance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the organization and settings for the objects:</td>
</tr>
<tr>
<td>&gt; S_USER_GRP (in particular: who can maintain which user groups?)</td>
</tr>
<tr>
<td>&gt; S_USER_PRO</td>
</tr>
<tr>
<td>&gt; S_USER_AUT</td>
</tr>
<tr>
<td>&gt; S_USER_ADM</td>
</tr>
<tr>
<td>&gt; S_USER_SAS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is the operating system level locked for the users?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; Use report RSPARAM to check the parameter rdisp/call_system. If the value is not set to 0, the operating system can be accessed from SAP ERP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is there an organizational division between application development, work scheduling and post processing, data input, operating, and archive management?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; Analyze in particular the assigned authorizations for the object S_TRANSPRT.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Was the program switch enabling use of the structural authorization always configured as specified?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; Check the use of the program switch for structural authorizations in the HCM module in table T77S0 (authorization main switch for HR).</td>
</tr>
</tbody>
</table>

| Was the authorization concept adequately tested before start-up? |
USER INTERFACE

Are the users specifically directed to the relevant sub-menu by means of a corresponding entry in the user master record?

> Call report RSUSR002, generate a list of all the users in question, click twice the ‘other view’ button, and check the ‘start menu’ column.

Does Customizing ensure that users only have access to the data they need to carry out their tasks?

> Use PA20 in Human Resources, for example, to check the masks (screens) that the individual users can access.

> Check the Customizing settings for the topic: „Customizing Interface“.

PROTOKOLLIERUNG

Is the user data logged by the operating system in such a way that it can be determined who outside SAP ERP has accessed which SAP ERP data, when, how, and with which resources?

Is the download logging function activated in the Security Audit Log?

Is the download log regularly evaluated with regard to data protection using SM20?

8.6.3.4 ITEM 4: TRANSFER CONTROL

According to item 4, it must be ensured that during electronic transfer, transporting, or storage on data carriers, personal data cannot be read, copied, modified, or removed without authorization and that it can be checked and established where a transmission of personal data is provided for by means of data transfer equipment (transfer control).

ACCESS PROTECTION

Are users/functions/rights assigned?

In addition to the overview of users in RSUSR002, is there also a table that identifies the current status of users and authorizations?

Is the user group differentiated in the authorization master record, that is, is it maintained by department or in relation to cost centers? Use RSUSR002 >Display all users> ‘other view’ to analyze the user groups.
## DATA TRANSFER

Is an overview/list kept of the departments where data transfer can be executed by programs?

| > Check for RFC, CPIC and ALE connections using the Audit Information System (SYSTEM AUDIT: SYSTEM CONFIGURATION – SYSTEM or – COMMUNICATIONS TYPE.) |
| > Check, as needed, access rights given to third parties (for example, external consultants or system maintenance). |

The System Audit is a component of the SAP ERP Basis Component, which means this audit function is available in mySAP™ systems in which the financial components are not active (for example, the Human Capital Management Systems).

Information about system settings, authorizations, as well as table values are essential elements of the Audit Information System – System Audit.

| Is there up-to-date documentation, external to the SAP ERP system, in accordance with Article 10, paragraph 4 of the German Federal Data Protection Act, on the programs to be used for automatic transfer? |

| Is there a secure log, external to the SAP ERP system, for automated transfer which records: |
| > The transferring users (sender) |
| > The recipients (receiver) |
| > The data |
| > The date |
| > The time? |

| Is the data encrypted using Secure Network Communications (SNC) or Secure Store & Forward (SSF) on the transfer routes? |

If so, between which instances?

| > SAP GUI and the application server? |
| > the application server and the printer? |
| > other? |
### OUTPUT MANAGEMENT

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is it documented which output can be redirected to PC?</td>
<td>&gt; Check the assigned authorizations for the object S_GUI (activity 61).</td>
</tr>
<tr>
<td>Is the output of printed material by the Personnel department user-related?</td>
<td></td>
</tr>
<tr>
<td>Are the printer authorizations configured with regard to the department or the user, or can copies be printed inadvertently in external departments/locations/countries (local printers)?</td>
<td>&gt; Check the authorizations for the object S_SPO_DEV and their assignment to users through roles or profiles.</td>
</tr>
</tbody>
</table>

### 8.6.3.5 ITEM 5: INPUT CONTROL

Fifthly, it must be ensured that subsequent checks can be made to establish whether and by whom personal data was entered, modified, or removed in data processing systems (input control).

### LOG SETTINGS

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which users are logged automatically?</td>
<td>&gt; Check the log filter definition in the Security Audit Log using transaction SM19.</td>
</tr>
<tr>
<td>&gt; Use report RSPARAM to check if the global setting for logging is set.</td>
<td>The system parameter rsau/enable should be set to 1.</td>
</tr>
<tr>
<td>Is the function for logging table changes activated?</td>
<td>&gt; Use RSPARAM and RECLIENT to check the rec/client and TP parameters.</td>
</tr>
<tr>
<td>Do the log reports for important table changes include changes to technical attributes of the tables (especially for system and key tables)?</td>
<td>&gt; List all the tables in question and check the settings (transaction SCU3 or display the table DD09L)</td>
</tr>
<tr>
<td>Is there a secure log which records the entries for all relevant SAP objects which includes:</td>
<td>&gt; the user who entered the data (name)?</td>
</tr>
<tr>
<td>&gt; the date and time of creation?</td>
<td>&gt; the data created?</td>
</tr>
<tr>
<td>&gt; Use transaction SCD0 to check the change documents set for all the objects in question.</td>
<td></td>
</tr>
<tr>
<td>Is anybody authorized to delete the change documents?</td>
<td>&gt; Use the User Information System (transaction SUIM and/or the report RSUSR002) to check which users have activity 06 for the object S_SCD0.</td>
</tr>
</tbody>
</table>
LOG ANALYSES

Which logs are activated in SAP ERP?

Which log contents in the SAP ERP system are used? By whom and for purpose?

> Is the Security Audit Log activated and why? Use report RSPARAM to check transaction SM19 and the rsau/enable parameter (value must be 1).

> Check the system log for failed logons (transaction SM21).

> Are the daily statistics (transaction STAD) used (if needed)? See the parameter stat/level = 1.

> Which application logs are activated? Compare the configuration SLG0 for the SLG1 (transactions).

> Who can use the function for logging workflows (transactions SWI2_xxx and SWI5), and for what purpose?

> For which business objects is logging activated? (transaction SCD0)?

> Logging tables (transaction SCU3)

> Check the change logs for users, profiles, and authorizations (transaction SUIM)

8.6.3.6 ITEM 6: ORDER CONTROL

Item 6 stipulates that it must be ensured that personal data to be processed for an external customer/contractee can only be processed in accordance with the instructions from that customer/contractee (order control).

ACCESS PROTECTION

Are users/functions/rights assigned for the contractor?

In addition to the overview of users in RSUSR002, is there also a table that identifies the current status of users and authorizations of the contractor?

Is the user’s user group differentiated in the authorization master record for the contractor, that is, is it maintained by department or in relation to cost centers? Use RSUSR002 ->Display all users -> ‘other view’ to analyze the user groups.

Are the contractor’s authorizations restricted to a minimum?

Is it ensured that adequate checks cover the risks of comprehensive authorizations for the contractor?
8.6.3.7 ITEM 7: AVAILABILITY CONTROL

Item 7 stipulates that it must be ensured that personal data is protected against accidental destruction or loss (availability control).

**ACCESS PROTECTION**

Are sufficient, regular backup runs provided?

Is it ensured at the operating system level that SAP files cannot be inadvertently deleted? Are the access rights restrictively assigned at the operating system level in accordance with SAP recommendations? Are the available access rights checked regularly?

Is it ensured at the database system level that SAP files cannot be inadvertently deleted? Are the access rights restrictively assigned at the database level in accordance with SAP recommendations? Are the available access rights checked regularly?

Is access to the archived data and data storage media adequately protected? Check the relevant organization.

Is it ensured that the data processing center and the data storage media are adequately protected against the effects of fire, water, power failure, and power fluctuations?

Is it ensured that the data storage media are adequately protected against the effects of material fatigue? Check whether there is adequate random sampling.

8.6.3.8 ITEM 8: DATA USAGE RESTRICTIONS

Item 8 stipulates that it must be ensured that data collected for separate purposes can be processed separately.

**ACCESS PROTECTION**

Are users/functions/rights for authorized purposes assigned strictly enough at the access protection level?

Check the access rights of individual user groups to:

- The program library
- Additional functions, such as ABAP Query and Ad Hoc Query
- The programming tools
- The administration functions
- The ABAP List Viewer in evaluation programs for personal data
- In particular, the logs and change documents
8 Appendix

OTHER MEASURES

Are the users/functions/rights adequately separated at the level of the individual systems, clients, and company codes?

Are the remaining risks covered by appropriately training the users in the departments, in programming, and in system management?

8.6.3.9 MISCELLANEOUS CHECKS

The introductory paragraph of the appendix to Article 9 of the German Federal Data Protection Act (BDSG) also requires that "the internal organisation of authorities or enterprises is to be arranged in such a way that it meets the specific requirements of data protection."

This requirement should be monitored by performing the following checks:

GENERAL GUIDELINES

Do data security guidelines exist (in general or especially for data processing), and are they up-to-date?

Are all the persons involved appropriately informed of these guidelines?

Are any investigations carried out following breaches of security?

Which logs have been created and by whom?

Does the procedure ensure that any lack of technical and organizational measures or breaches of data protection are immediately forwarded to the person responsible for data protection in the company and that corrective action can be taken in conjunction with this person?

Has a risk and vulnerability analysis been carried out?

ACCESS MANAGEMENT AND LOG ANALYSES

Are the access authorizations of a user who is leaving the company or who is to be transferred elsewhere deleted immediately?

Is there an automatic workflow for deleting users (as needed)?

Is the automatic administration and maintenance of user master records, authorizations, profiles, and, if applicable, roles executed in an adequate and timely manner?

> Check the authorization framework concept and the organizational management of user administration, as well as the maintenance of profiles, authorizations, and roles.
### ACCESS MANAGEMENT AND LOG ANALYSES

<table>
<thead>
<tr>
<th>Question</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the auditability of access authorizations taken into consideration?</td>
<td></td>
</tr>
<tr>
<td>Does the internal control system regularly check the compliance with the authorization concept? How often are such checks performed?</td>
<td></td>
</tr>
<tr>
<td>Are there any sanctions governing identified misuses and attempts to misuse systems?</td>
<td></td>
</tr>
<tr>
<td>Is the logging of user logons and password changes (report RSUSR006) checked regularly?</td>
<td></td>
</tr>
<tr>
<td>Is the delivery of printouts to users without local/office printers regulated?</td>
<td></td>
</tr>
<tr>
<td>Are the authorizations to access printers sufficiently restricted?</td>
<td></td>
</tr>
<tr>
<td>Is the backup procedure at the database level documented in writing?</td>
<td></td>
</tr>
<tr>
<td>Have the backup files been protected by a password or a release date, for example?</td>
<td></td>
</tr>
<tr>
<td>Are the configured protective measures regularly subjected to a thorough test to establish whether they still sustain the desired level of protection?</td>
<td></td>
</tr>
</tbody>
</table>