

Notes on Data protection and Anonymization SAP Test Data Migration Server 4.0 (SAP TDMS 4.0)



Version 2.2

August 2012



[Copyright]

© Copyright 2012 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Typographic Conventions

Type Style	Description
<i>Example text</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
Example text	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

History of Changes

The Notes on Data Protection is regularly updated on *SAP Service Marketplace* at <https://service.sap.com/tdms>.



Make sure you have the latest version of the Notes on Data Protection by checking *SAP Service Marketplace*.

The following table provides an overview of the most important changes that were made in the latest versions.

Notes Version	Important Changes
1.0	First version of the document
2.0	p. 6 "Data protection officers" added to target audience p. 6 Chapter "Responsibility" added p. 6 chapter "Validity of data processing" changed to "Legitimacy of Data Processing". Content of chapter changed p. 7 Chapter "Notification requirement" added p. 7 Changes in chapter "Data Transfer"; recommendation added for mobile devices. p. 7 / 8 Chapter "Data avoidance, data economy" separated into two chapters and content changed p. 8 Changes and additions in chapter "Anonymization/Pseudonymization of Data" p. 8 Chapter "Delete/Block" sentence added p.9 Chapter "Technical and Organizational Data Protection Measures" sentence added
2.1	New Version created / Date changed from June to July 2012 p. 6 change in "Legitimacy of Data Processing" p. 8 change in "Purpose limitation and transparency" p. 8 change in "Anonymization/Pseudonymization of Data" p. 8 change in "Delete/Block" p. 9 change in "Rights of the parties concerned" p. 9 sentence added to "Technical and Organizational Data Protection Measures"
2.2	New Version created / Date changed from July to August 2012 P 8. Change in "Anonymization/Pseudonymization of Data"

CONTENTS

Introduction.....	6
Target Audience.....	6
Notes on Data Protection with TDMS	6
Legitimacy of Data Processing	6
Notification requirement.....	7
Special categories of Data.....	7
Data Transfer	7
Data Avoidance and Data Economy	7
Purpose limitation and transparency	7
Anonymization/Pseudonymization of Data	8
Delete/Block.....	8
Rights of the parties concerned	9
Technical and Organizational Data Protection Measures	9
Project Requirements for the Anonymization of Data with TDMS.....	10
Scrambling.....	10
Customer Objects.....	10



Introduction



Legal Disclaimer

SAP cannot give you a binding legal advice, please contact your legal department.



This guide does not replace the daily operations handbook that we recommend customers should create for their specific day-to-day operations.

Target Audience

- Consultants
- Security specialists
- System administrators
- Data protection officers

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.



Notes on Data Protection with TDMS

Legal Disclaimer

SAP AG cannot give you a binding legal advice, please contact your legal department.

In this document, we have compiled some notes on data protection that you should consider when setting up and using TDMS.

Responsibility

As the controller, you are responsible for complying with the various data protection regulations when using TDMS. Regarding to directive EC 95/46 within the European Union, a controller is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The controller stays responsible, even if another body processes personal data on behalf of him.

Legitimacy of Data Processing

As far as you process personal data using TDMS, the legitimacy of the data collection, processing, and usage must be in accordance with the law applicable to your company or institution. For example, directives 95/46/EC, 2002/58/EC, or 2000/31/EC have to be considered as general conditions for data protection within the European Union. Also national regulations applicable for your company or institution must be considered

Regarding to directive EC 95/46 personal data are any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

these include e.g. customer or user data, employee data or log protocols, which are processed to monitor the security of the IT systems.

Please note, that data processing can be permitted if it is based on the consent of the person concerned or a legal regulation. This includes log data relating to an identified or identifiable natural person.

Check before you process data with TDMS whether your data is allowed to be processed in compliance with the relevant data protection legislation.

Notification requirement

Please bear in mind that in some countries it is mandatory to appoint an operational data protection officer, who, if necessary, has to evaluate the TDMS system in terms of data protection for your company in advance. Furthermore, it may be necessary, depending on the legal situation, to list the TDMS system in a legally prescribed system register and document the data processing. It may also be necessary to notify official bodies.

If in doubt, contact your data protection officer or the relevant supervisory authority.

Special categories of Data

Special categories of data include details about the racial and ethnical origin, political opinions, religious or philosophical conviction, trade union membership, health or sex life. If it is not possible to rule out during the usage of TDMS that these details will be processed, note that this generally may only be used for certain specified purposes and usually requires consent (see above). In addition, special laws or legal norms can stipulate further requirements, which can also refer to additional data depending on the industry.

Data Transfer

The transfer of data between different places must be based on consent or a legal regulation. Especially the transfer of personal data from locations within the EU or EEA to third countries must comply with Art. 7 and Art. 25 of the directive EC 95/46. Therefore, the third country in question must ensure an adequate level of protection.

According to directive EC 95/46, there is no “intra group exemption”. A permissive standard is required even for a data transfer between group companies. Companies with headquarters in the EU or EEA (e.g. Germany), who transfer their data to locations within the EU or EEA, can assume that there is an adequate level of data protection. However, this is different for third countries so that a special authorization may be necessary for such a data transfer. This can be participation in the “Safe Harbour” standard in the United States, concluding standard contractual clauses of the European Commission, or an officially recognized data protection guideline across the group (Corporate Binding Rules).

We recommend that you use encryption to secure mobile storage against unauthorized usage. Ensure that the use of mobile storage devices is in line with corporate regulations and guidelines and consult with the departments related to data protection in advance.

Data Avoidance and Data Economy

TDMS can be individually adapted to the requirements of your company or institution. The institution must orientate itself to the principles of data economy and data avoidance and as far as possible not include any sensitive data. Then only process as little personal data as possible and only as much as necessary.

Please note, that data quantity can be reduced using TDMS according to the requirements.

Purpose limitation and transparency

The processing of data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. The purposes must be explicit and legitimate and must be determined at the time of collection of the data; the purposes of processing data

further to collection shall not be incompatible with the purposes as they were originally specified. By this means, type and quantity of data to be processed with TDMS has to be defined before using TDMS. Please bear in mind, that using authentic personal data for testing usually changes the origin purpose.

At any rate, the person concerned must be informed about the identity of the controller, type, purpose, and scope of data processing.

For data processing using TDMS, we recommend setting out some guidelines to guarantee compliance with the data protection regulations.

Anonymization/Pseudonymization of Data

Additionally, make use of the possibilities of pseudonymization and anonymization.

If data is rendered anonymous in such a way that the data subject is no longer identifiable, data protection law is not applicable.

Pseudonymization describes the replacement of names or other characteristics through distinguishing marks to make identification impossible or much more difficult

For this purpose TDMS offers different methods (see SAP Guideline "How to scramble Data Using SAP Test Data Migration Server")

In combination with an adequate wide dataset or further restrictions it is possible to anonymize data with the following scrambling methods:

- Random Selection
- Random Table for Time Periods
- Fixed Value
- Number Conversion

For pseudonymization of data it is possible to use

- Manual 1:1 Mapping.

You can also combine „Value Range Table“ with different scrambling methods to anonymize or pseudonymize data.

Please check all scrambling methods, to make sure, that in particular anonymization or pseudonymization is effectively given for your data.

Since sensitive data is present in the production system, we recommend that you scramble the data before data transfer to the non-production system. It may be against the law not to anonymize or pseudonymize personal data by using TDMS, e.g. by using personal data for testing.

If you choose not to use any scrambling-methods, TDMS will give a warning by pop-up message. Please check, if your selection is lawful.

Delete/Block

Note that different periods apply regarding the retention of personal data. In principle, all data is to be deleted as soon as it is no longer necessary for the purpose for which it was collected. This includes also log data relating to an identified or identifiable natural person.

If data cannot be deleted, instead of a deletion, a blocking could be done.

TDMS sends personal data to a receiver system and saves it there. Note the guidelines that apply to your company or institution.

Rights of the parties concerned

Note that the persons concerned by the data processing using TDMS have different rights depending on the legislation. In principle, this can include the following rights:

- The right of access, the right to notification and information,
- The right to the correction, deletion, and blocking of data, or
- The right to withdraw consent to data processing.

Inform your users about the relevant data protection laws.

Technical and Organizational Data Protection Measures

Make technical and organizational measures for data protection when using TDMS:

- Define which employees have authorization for which activities in the system.
- Regularly check that the authorization concept is adhered to.
- Do not pass on any data to unauthorized persons.
- If you employ external service providers for data processing or maintenance and support of data processing, act in compliance with the legal rules for contractual processing of personal data.
- Use the password protection and do not transfer any personal data unencrypted on the internet.
- Require your employees to comply with data protection requirements and inform them about them.
- Regularly contact your data protection officer, particularly in case of doubt.

The measures have to be reasonable and proportionate to the protection requirements of the data.

Please note, that the protection level depends on the personal data being processed. It may be necessary to improve the technical and organizational measures to achieve an adequate degree of data protection.



Project Requirements for the Anonymization of Data with TDMS

TDMS 4.0 is a tool that supports the anonymization of data (scrambling) within SAP software components.

Scrambling

The scrambling functionality in TDMS 4.0 consists of:

1. A special environment for the development of scrambling rules which can be used directly in TDMS.

Rules can be developed independently of the SAP software component and assigned to ABAP Dictionary objects at table and field level. There are various supporting functions, which explain the development. The development programming language is ABAP.

2. Predefined scrambling rules that are delivered with TDMS 4.0 and can be used directly in different TDMS scenarios.

Since the SAP software components are used by customers in many different ways and are often extended by standard enhancements (for example, industry solutions) and customer enhancements, predefined rules can often only be used as templates and must also be assigned to Dictionary objects from enhancement components.

The anonymization requirements of the customers are often very different. Depending on the type of anonymization, for example, of an address, follow-on processes can possibly no longer be performed because the logical relationship between the address fields is lost during the anonymization. On the other hand, an anonymization fails, when the logical relationship to a person can be identified.

In this area of conflict, customers are deciding in favor of individual scrambling rules which must then be developed with TDMS in the customer project.

Customer Objects

If TDMS scrambling is used in customer projects, the customer expects that the anonymization of data meets the applicable data protection regulations. If the anonymized data should be used for tests, logical relationships between anonymized objects must be retained since otherwise the processing is incorrect.

The following prerequisites must be met:

1. The tool used for the anonymization must enable an anonymization which meets the applicable data protection regulations. A reidentification of the anonymized data must only be possible with a disproportionately high effort (concept of de facto anonymity).

This is possible with TDMS since in principle all data of the SAP database can be anonymized. The TDMS development environment provides supporting functions for the complete and consistent application of scrambling rules.

2. The customer must define his test requirements and derive from them which rules are necessary for the anonymization. Either predefined rules from TDMS can be used or new rules can be developed with the TDMS development environment.

Therefore, the main focus is to be put on the conception phase and the reconciliation with the persons responsible for data protection at the customer. A case-by-case conception of the test objective with the resulting derivations of the dataset to be used should be created. Rules on the legality of the data processing, confidentiality, and aspects of data minimization should be considered in the relevant conception.

Special considerations of different industry sectors must also be taken into consideration.

3. The persons responsible for the implementation of anonymization rules normally have information about the way in which data is anonymized.

To meet data protection regulations, data protection must therefore be ensured by additional organizational measures. This includes both an authorization concept and nondisclosure agreements for the persons involved in the anonymization.