Kurzgutachten zum IT Produkt

Test Data Migration Server (TDMS) 4.0

1. Name und Version des IT Produkts:

IT Produkt: Test Data Migration Server (TDMS), Version 4.0

2. Hersteller des IT Produkts:

Firmenname : SAP AG

Firmenadresse: Dietmar-Hopp-Allee 16,
69190 Walldorf

Web: www.sap.com

Ansprechpartner: Volker von Seggern

3. Zeitraum der Evaluation:

27.02.2011 – 06.09.2012

4. EuroPriSe Experten, die das IT Produkt evaluiert haben:

Name der rechtlichen Expertin: Dr. Irene Karper

Adresse : datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen, Deutschland

ikarper@datenschutz-cert.de

Name des technischen Experten: Ralf von Rahden

Adresse: datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen, Deutschland

rrahden@datenschutz-cert.de

5. Zertifizierungsstelle:

Name: Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig Holstein

Adresse: Holstenstr. 98
24103 Kiel, Germany

E-Mail: europrise@datenschutzzentrum.de

6. Spezifikation des Evaluationsgegenstands (ToE):

Gegenstand der Evaluierung (ToE) ist das IT-Produkt *Test Data Migration Server (TDMS) in der Version 4.0* (nachfolgend TDMS).

Zum ToE gehören die folgenden Komponenten

- TDMS-Plug-in auf einem Sendesystem
- TDMS-Server, bestehend aus zentralem System und Kontroll-System
- TDMS-Plug-in auf einem Empfängersystem.

7. Generelle Beschreibung des IT Produkts:

TDMS ist eine Erweiterungssoftware für SAP-Systeme aus den SAP-Produkt-Linien „Business Suite“, „Industry Solutions“ und „SAP NetWeaver BW“.

Mittels TDMS werden Daten aus SAP Systemen für Entwicklung, Tests, Qualitätssicherungen oder Schulungen zur Verfügung gestellt. Dabei kann der Anwender die Datenmenge einerseits auf das Notwendigste reduzieren. Andererseits können Daten verfälscht (gescrambled) werden, ohne dass die Konsistenz verloren geht.

7.1 Zweck und Einsatzbereich

TDMS erlaubt die Verarbeitung von Daten des jeweiligen SAP-Basissystems, wobei durch verschiedene, vom Anwender in jedem Einzelfall auszuwählende Regeln zur Verfremdung der Daten (Scrambling) die Identifizierbarkeit von Personen vollständig verhindert (Anonymisierung) oder zumindest erschwert werden kann (Pseudonymisierung). Als Ausnahme ist es dem Anwender allerdings auch möglich, eigene Regelungen zu definieren, in denen weder eine

Anonymisierung, noch eine Pseudonymisierung stattfindet. Um den Anwender für jeden Fall auf die Einhaltung des Datenschutzes zu sensibilisieren, erscheint zuvor ein Popup mit einem Warnhinweis, sofern der Anwender keine Scrambling-Regeln verwendet und die Daten folglich unverfremdet genutzt werden. Zudem wird der Anwender in einem Merkblatt auf die Aspekte Datensparsamkeit, Anonymisierung und Pseudonymisierung hingewiesen.

Bei der Anwendung von TDMS werden zudem administrative Daten (Protokolldaten) über das SAP-Produktivsystem erfasst und können dort zur Revisionskontrolle, verarbeitet werden. TDMS erzeugt für jede Aktivität ein eigenes Log. Dieses enthält den Benutzernamen des Anwenders bzw. Benutzers als einziges personenbezogenes Datum. TDMS übergibt die Logdaten an das SAP-Produktivsystem ohne sie in TDMS zu speichern.

Anwender sind Unternehmen oder öffentliche Stellen. Typischer Weise handelt es sich bei den über TDMS verarbeiteten Daten um Personaldaten, wie sie im SAP-Modul Human Capital Management (HCM) anhand der Info-Typen angelegt werden, oder um Kundendaten, wie sie in den Modulen Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) oder Business Intelligence (BI) hinterlegt werden.

TDMS in der Version 4.0 kann bei folgenden SAP-Basissystemen eingesetzt werden:

- Business Suite:
  - SAP ERP
  - SAP ERP HCM
  - SAP CRM
  - SAP SCM
  - SAP SRM
- Industry Solutions:
  - AFS

- Banking (Loans and Deposits)
- Oil & Gas (Downstream)
- Utilities
- CRM for Utilities
- Healthcare
- DIMP
- Retail

- SAP NetWeaver BW
- SAP GTS.

7.2 Funktionsumfang in der auditierten Standardausführung

Das Produkt TDMS besteht aus folgenden Komponenten:

- TDMS-PlugIn auf dem Sendesystem
- TDMS-Server, bestehend aus zentralem System und Kontroll-System
- TDMS-PlugIn auf dem Empfängersystem.

Die Systemlandschaft, in der TDMS angewandt werden kann, besteht aus einem Sendersystem (Sender), dem TDMS-Server (bestehend aus einem Kontrollsystem (Control) und einem Zentralen System (Central), sowie einem Empfängersystem (Receiver).

TDMS erhält für Entwicklung, Tests, Qualitätssicherungen oder Schulungen vom Anwender ausgewählte Echtdaten aus einem Sendersystem. Das Sendersystem ist immer ein SAP-Produktivsystem. Die ausgewählten Echtdaten können mittels TDMS auf dem SAP-Produktivsystem verfremdet (gescrambelt) werden. TDMS bietet dem Anwender hierfür verschiedene Mechanismen. Das Scrambling ist der Regelfall, da dies ein wesentlicher Vorteil von TDMS ist. Gleichwohl ist es möglich, ausgewählte Daten auch ohne Verfremdung an das Empfängersystem weiterzugeben.

Im Kontrollsystem des TDMS-Servers sind die Scrambling-Mechanismen und Einstellungen (verwendete Systeme, angelegte Benutzer, definierte Rollen, Berechtigungen) hinterlegt. Im Zentralen System wird die Hintergrund-Verarbeitung der Daten-Migration durchgeführt.

Wird ein Vorgang angestoßen, werden die Daten auf das Empfängersystem weitergeleitet.

Scrambling

Im Fokus von TDMS steht das Scrambling der Daten, bevor diese aus dem Sendesystem an das Empfängersystem übermittelt werden. Der Anwender kann hierfür Regelungen definieren oder - speziell für SAP ERP HCM - vom Hersteller vordefinierte Scrambling-Pakete nutzen und diese für seine Bedürfnisse anpassen. Dabei bietet das Scrambling die folgenden Möglichkeiten:

- Datenwerte können zufällig verändert, fest vergeben oder gelöscht werden
- Verfremdungsstrategien für einzelne Datenfelder können an andere Datenfelder weitervererbt werden. Auf diese Weise bleibt die Konsistenz des Datensatzes erhalten.

Ob die Verwendung bestimmter Scrambling-Regeln zu einer Anonymisierung bzw. Pseudonymisierung im Sinne des Datenschutzrechts führt, ist vom Anwender in jedem Einzelfall genau zu prüfen.

Soweit der Anwender TDMS ohne die Verfremdung von Echtdaten nutzt (z.B. um eine 1:1-Kopie der Daten zu erstellen), wird er systemseitig durch ein Pop-Up-Fenster darauf hingewiesen, dies zu überprüfen. Ferner wird der Anwender in einem Hinweisblatt zum Datenschutz („Notes on Data protection and Anonymization SAP Test Data Migration Server 4.0 (SAP TDMS 4.0)“ auf die Beachtung von Datenschutzbestimmungen sensibilisiert.

Datenreduktion

TDMS ermöglicht es ferner, z.B. nur einzelne Buchungskreise oder Daten bestimmter Zeiträume auszuwählen. Hierdurch können Daten auf das Notwendigste reduziert werden.

Datentransfer

Der Datentransfer erfolgt direkt vom Sende- zum Empfängersystem über Remote Function Call (RFC). Alternativ ist auch eine Übertragung über eine Export- / Importfunktion möglich. Dabei wird der erzeugte Cluster der gescrambelten Daten, sofern Scrambling-Regeln angewendet worden sind, in eine Datei exportiert, die mit Hilfe eines mobilen Datenträgers im Empfängersystem importiert werden kann. Da die Daten auf diesem Wege nicht auf die gleiche Weise geschützt sind, wie unter Verwendung der RFC-Verbindungen, werden Anwender in Kapitel 3.11 des Master Guides darauf hingewiesen, Daten z.B. durch Verschlüsselung zu schützen.

Hervorzuheben ist, dass personenbezogene Daten zu keinem Zeitpunkt auf dem Zentralen System oder dem Kontrollsystem von TDMS gespeichert werden. Stattdessen erfolgen ein lesender Zugriff auf das Sendersystem und ein schreibender Zugriff auf das Empfängersystem. TDMS unterstützt in diesem Sinne lediglich die Weitergabe der Daten.

7.3 Funktionsumfang außerhalb des auditierten Standardumfangs

Nicht zum Funktionsumfang und damit nicht zur Evaluation gehören

- das Sendesystem sowie das Empfängersystem, soweit dieses nicht identisch ist mit dem TDMS-Server
- die beim Anwender zugrundeliegende SAP-Produktlinie oder das SAP-Basissystem inklusive der Datenerfassung und Datenverarbeitung
- die Einsatzumgebung beim Anwender sowie eine Datenverarbeitung im Auftrag des Anwenders
- die Hardwarebestandteile der Server von TDMS, das Betriebssystem und das eingesetzte Datenbanksystem

- die Lizenzierung und Vertriebsprozesse bei der SAP AG oder deren Kunden.

8. Transnationale Aspekte:

TDMS kann von Unternehmen oder öffentlichen Stellen mit Niederlassungen innerhalb der Europäischen Union, des EWR oder weltweit eingesetzt werden. Datenbank und Server befinden sich dabei im Verantwortungsbereich des jeweiligen Anwenders. Die einschlägigen Rahmenvorgaben finden sich vor allem in der Richtlinie 95/46/EG[1]. Diese sind in den EU-Mitgliedstaaten in das nationale Recht umgesetzt worden, wie etwa in das deutsche Bundesdatenschutzgesetz (BDSG)[2]. Zudem sind die Auslegungshilfen der Art-29-Datenschutzgruppe, die Rechtsprechung der Europäischen Gerichtshöfe sowie nationale Vorgaben der Datenschutzaufsichtsbehörden zu beachten, wie z.B. die für die Bundesrepublik Deutschland geltende Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

9. Tools, die der Hersteller und Anbieter des IT Produkts nutzt:

---

10. Edition des EuroPriSe Kriterienkatalogs:

Die Experten nutzen den EuroPriSe Kriterienkatalog in der Version aus Mai 2011 und das EuroPriSe Glossar in der Version 1.0.

11. Evaluationsergebnisse:

Folgende wesentlichen Prüfergebnisse wurden festgestellt:

11.1 Umsetzung von rechtlichen Anforderungen

Welche Rechtsgrundlage für die Anwendung von TDMS in Betracht kommt, hängt vom jeweiligen Zweck der Datenverarbeitung und den für den Anwender einschlägigen Rechtsvorschriften ab. TDMS unterstützt dies, indem der

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl.EU L 281 v. 23.11.1995, S. 31ff.
2 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung v. 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes v. 14.08.2009 (BGBl. I S. 2814).

Anwender in den Hinweisen zum Datenschutz darauf hingewiesen und sensibilisiert wird, die Rechtskonformität generell zu überprüfen.

Zudem ermöglicht TDMS eine Auswahl, Reduktion oder das Verfremden der zu transferierenden Daten, so dass der Anwender auch nur solche Daten auswählen kann, die der jeweiligen Grundlage entsprechen. Sofern mittels TDMS zudem Daten anonymisiert werden, ist die Rechtmäßigkeit der Datenverarbeitung grundsätzlich gegeben.

Ebenfalls werden die Anforderungen an Transparenz, Zweckbindung und Verhältnismäßigkeit adäquat erfüllt. Insbesondere die Hinweise zum Datenschutz sowie weitere von der SAP AG zur Verfügung gestellte Dokumentationen ermöglichen einen Überblick über die mittels TDMS verarbeiteten Daten und Prozesse für eine weitere datenschutz-relevante Bewertung und unterstützen so die Aufgaben des betrieblichen Datenschutzbeauftragten.

11.2 Datensparsamkeit

TDMS bietet die Möglichkeit, nur solche Daten zu verwenden, die für die jeweilige Verarbeitung notwendig sind. Zugleich können personenbezogene Daten in optimaler Weise anonymisiert oder pseudonymisiert werden. Temporäre Daten werden umgehend gelöscht.

Von TDMS erzeugte Sekundärdaten werden an das zugrunde liegende SAP-System auf dem TDMS-server übergeben, ohne eine Löschfrist für diese zu setzen. Dies ist mit dem nächsten support package bis spätestens März 2013 zu ändern.

Der Anwender wird durch das Merkblatt auf die Einhaltung der Grundsätze der Datenvermeidung und Datensparsamkeit explizit hingewiesen und aufgefordert, diese bei der individuellen Einrichtung und Nutzung des Systems zu beachten.

11.3 Datensicherheit

Berechtigungen können entsprechend der Rollen und Funktionen abgestuft zugewiesen werden. TDMS wird mit vordefinierten Rollen ausgeliefert, wobei diese differenziert vom Anwender angepasst werden können. Hierdurch

unterstützt TDMS die Einrichtung eines fein-granularen Berechtigungs- und Rollenkonzepts.

TDMS wird als Erweiterung eines bestehenden SAP-Basissystems installiert. Dabei nutzt es die Authentisierungsmechanismen des Basissystems. Der Benutzer muss sich gegenüber dem System unter Nutzung eines dieser Systeme anmelden. Nur ein Nutzer, der mit entsprechenden Rechten konfiguriert worden ist, erhält entsprechenden Zugriff auf TDMS. Eine Passwortrichtlinie zur Festlegung der Passwortkomplexität muss im Basissystem festgelegt werden und hängt von der Risiko-Analyse des Anwenders für seine Daten ab.

Insgesamt bietet TDMS eine detaillierte Protokollierungsfunktionalität, die zusammen mit den dazugehörigen Berechtigungen vom Anwender nach seinen Bedürfnissen konfiguriert werden kann und muss.

In TDMS werden die Verbindungen zwischen Sender-, Zentral- und Empfängersystem über RFC-Verbindungen realisiert. Die RFC-Verbindung lässt sich mittels Secure Network Communication (SNC) verschlüsselt gestalten, etwa unter Verwendung von SSL. Bei Verwendung verschlüsselter RFC-Verbindungen werden die Autorisierungs-Credentials natürlich auch verschlüsselt und somit geschützt übertragen.

TDMS selbst schützt die Netzwerkverbindungen nicht, unterstützt aber den Einsatz sicherer Protokolle.

In TDMS werden grundsätzlich keine Primärdaten dauerhaft gespeichert. Es besteht daher nicht die Notwendigkeit Daten zu sichern oder vor unvorhergesehenem Verlust zu schützen. Für Backup und Restore wird im Operation Guide auf die allgemeine Dokumentation von SAP Netweaver verwiesen. TDMS bietet hierzu keine Funktionalität an.

Im Operation Guide wird der Anwender über möglichen Support informiert. Etwa kann ein interner Support Desk eingerichtet werden oder Anfragen/Problemmeldungen können über eine CA-TDM-Komponente direkt an SAP weitergeleitet werden. Der Entwicklungsprozess von TDMS folgt dem PIL

(Product Innovation Life Cycle). Im PIL sind klar definierte Test und Freigabe-Verfahren definiert, die eine sorgfältige Qualitätssicherung gewährleisten.

TDMS selbst stellt keine Verschlüsselungsfunktionen zur Verfügung. Da TDMS für eine Übertragung im selben Netzwerk konzipiert wurde, ist dies aus Sicht der Gutachter auch nicht notwendig.

Über eine Exportfunktion können ausgewählte und gescrambelte Daten für die Übertragung auf einen mobilen Datenträger gespeichert werden. Für diesen Fall wird im Master Guide darauf hingewiesen, dass eine angemessene Verschlüsselung des Datenträgers dringend empfohlen wird. Ferner befindet sich im Merkblatt zum Datenschutz ein entsprechender Hinweis auf die Verschlüsselung mobiler Datenträger.

11.4 Umsetzung der Betroffenenrechte

TDMS unterstützt die Betroffenenrechte bei korrekter Systemeinrichtung und -nutzung durch den Anwender insgesamt adäquat. So wird der Anwender in den Hinweisen zum Datenschutz auf die Umsetzung von Betroffenenrechten bei der Nutzung von TDMS sensibilisiert. Zudem werden dem Anwender Produktunterlagen zu TDMS und Leitfäden zum Datenschutz für bestimmte SAP-Produktivsysteme zur Verfügung gestellt, die ihn ebenfalls auf den Umgang mit Betroffenenrechten sensibilisieren.

12. Datenfluss:

Der Datenfluss lässt sich mit folgender Grafik darstellen:

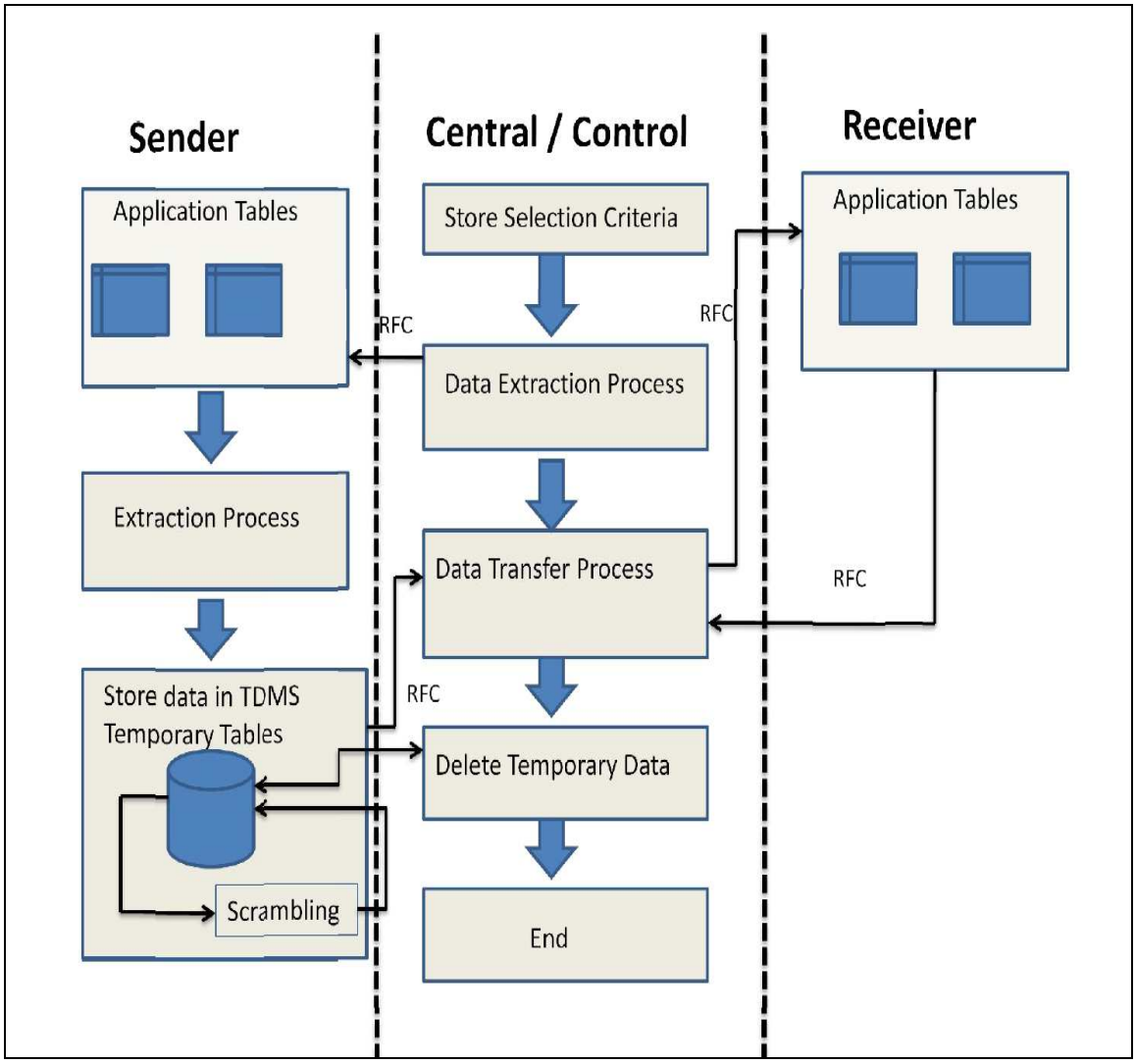

Abb. 1: Datenfluss

13. Funktionen zur Förderung des Datenschutzes:

Das Produkt enthält folgende, den Datenschutz fördernde Funktionen:

- TDMS bietet die Möglichkeit, hochwertige Testdaten aus Produktivdaten zu erstellen, während unnötige personenbezogene Daten in optimaler Weise anonymisiert oder pseudonymisiert werden können.
- Möglichkeiten der Datenvermeidung und Datenminimierung sind hervorragend. Die sofortige Löschung temporärer Daten auf dem Sendesystem nach dem Transfer sind beispielhaft.
- Anwender werden auf verschiedene Art und Weise auf die Anforderungen der Datenverarbeitung personenbezogener Daten hingewiesen, insbesondere auf die Möglichkeiten und Anforderungen der Anonymisierung und Pseudonymisierung. Hervorzuheben sind insoweit die im Datenschutz-Merkblatt zusammengefassten Hinweise zum Datenschutz.
- TDMS besitzt ein feingranulares Rollenkonzept. Es ermöglicht dem Anwender die mit ausgelieferten Rollen-Templates nach seinen Bedürfnissen genau anzupassen. Auf diese Weise können genau auf das Notwendigste eingeschränkte Berechtigungen vergeben werden.
- Das Incidentmanagement sowie Tests- und Freigabeverfahren sind exzellent.

14. Aspekte, die der Anwender besonders beachten sollte:

Die Datenschutz-konforme Nutzung von TDMS obliegt der Verantwortung des Anwenders. Er muss die ihm zur Verfügung gestellten Informationen des Herstellers zu den Datenschutzstandards und eine den Datenschutz fördernden Konfiguration in jedem Einzelfall anwenden.

Im Rahmen der Evaluation wurde festgestellt, dass die von TDMS erzeugten Log-Daten ohne vorgegebene Löschfrist an das SAP-Basis-System weitergegen werden. Der Nutzer wird in diesem Fall nicht durch den TOE bei der Einhaltung von Löschfristen unterstützt. Mit dem nächsten support package für TDMS wird ein Höchstalter von Logdaten von einem Jahr als Standardwert implementiert.

15. Kompensierung von Schwachpunkten:

TDMS erfüllt keine Anforderung der Evaluation mit der Bewertung “noch bestanden”.

Mangels Schwachpunkten muss nichts kompensiert werden.

16. Ergebnistabelle zu den wesentlichen Anforderungen:

EuroPriSe Anforderung	***Entscheidung***	***Bemerkung***
Datenvermeidung und Datenminimierung	exzellent	TDMS bietet die Möglichkeit, nur solche Daten zu verwenden, die für die jeweilige Verarbeitung notwendig sind. Zugleich können personenbezogene Daten in optimaler Weise anonymisiert oder pseudonymisiert werden. Temporäre Daten werden umgehend gelöscht.
Transparenz	exzellent	Die Dokumentation und Hinweise zu den rechtlichen Voraussetzungen und zum Datenschutz sind informativ, aktuell und verständlich.
Technisch-organisatorische Aspekte	exzellent	Das Rollen- und Berechtigungskonzept kann in optimaler Weise konfiguriert werden. Incidentmanagement, Tests- und Freigabeverfahren sowie die Hinweise zum Datenschutz mit Beispielen zur Datensicherheit sind vorbildlich und fördern die Umsetzung angemessener technisch-organisatorischer Aspekte beim Anwender.
Betroffenenrechte	adäquat	Der Anwender wird in den Hinweisen zum Datenschutz angemessen auf die Umsetzung von Betroffenenrechten bei der Nutzung von TDMS sensibilisiert.

Erklärung der Experten

Wir bestätigen, dass das oben genannte IT Produkt gemäß den EuroPriSe Kriterien, Regelungen und Prinzipien evaluiert wurde, und dass die vorgefundenen Ergebnisse, wie oben beschrieben, die Ergebnisse dieser Evaluation sind.

Bremen, 06.09.2012 Dr. Irene Karper LLM.Eur.

Ort, Datum	Name der rechtlichen Expertin	Unterschrift

Bremen, 06.09.2012 Ralf von Rahden

Ort, Datum	Name des technischen Experten	Unterschrift

Ergebnisse der Zertifizierung

Das oben genannte IT Produkt hat die Evaluation gemäß EuroPriSe bestanden.

Hiermit wird zertifiziert, dass das oben genannte IT Produkt den Gebrauch des Produktes oder des Services in der Weise fördert, dass es konform zu europäischen Regelungen zum Datenschutz und zur Datensicherheit eingesetzt werden kann.

Kiel 2012 Unabhängiges Landeszentrum für Datenschutz

Ort, Datum	Name der Zertifizierungsstelle	Unterschrift