Rechtliches und Technisches

Rezertifizierungsgutachten

Einhaltung datenschutzrechtlicher Anforderungen
durch das IT-Produkt

- SQS®-Testsuite für SAP® HCM -

der
SQS Software Quality Systems AG, Stollwerckstraße 11, 51149 Köln

erstellt von:

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen

email ab@datenschutzkontor.de

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)

Neustadt 56
24939 Flensburg

email sh@datenschutzkontor.de

Stand:
April 2008

Inhaltsverzeichnis

A. Einleitung

1 Das IT-Produkt SQS-Testsuite für SAP HCM (nachfolgend: SQS-Testsuite) der SQS Software Quality Systems AG (nachfolgend: SQS AG) ist bereits im Jahr 2003 vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) für das Gütesiegel für IT-Produkte des Landes Schleswig-Holstein zertifiziert worden.

2 Im Zuge einer geplanten Rezertifizierung ist das IT-Produkt des Antragstellers in Augenschein genommen und einer rechtlichen und technischen Begutachtung unterzogen worden. Ausgangspunkt und Grundlage der Begutachtung im Rahmen der Rezertifizierung war das Gutachten des Erst-Sachverständigen (T-Systems GEI GmbH, Business Unit ITC Security, Stefan Morkovsky, Rabinstraße 8, 53111 Bonn) vom 05.03.2003 (Version 1.1). Soweit die unterzeichnenden Sachverständigen für erforderlich gehalten haben, sind ergänzende Hinweise zu einzelnen Punktes des Anforderungskataloges gemacht worden; ansonsten sind im Rahmen der Rezertifizierung nur die Änderungen an dem Verfahren aufgezeigt und geprüft worden.

3 Wesentliche Änderungen des Verfahrens sind seit der Erstzertifizierung nicht vorgenommen worden. Das Verfahren ist lediglich an die jeweils aktuelle SAP-Software angepasst worden, ferner sind die eingesetzten systematischen Testmethoden weiter optimiert worden. Die Änderungen haben keinerlei datenschutzrechtliche Relevanz.

4 Dem Gutachten wird der Anforderungskatalog in der Version 1.2 zu Grunde gelegt.

B. Zeitpunkt der Prüfung

5 Die Prüfung des Verfahrens fand von 07.04.08 bis 11.04.08 statt.

C. Detaillierte Bezeichnung des Begutachtungsgegenstandes

6 Diesbezüglich wird weitestgehend auf das Erstgutachten verwiesen.

7 Bezüglich der Bezeichnung des Produktes ist darauf hinzuweisen, dass die SAP AG seit kurzem SAP HR in SAP HCM (Human Capital Management) umbenannt hat. Daher soll auch das Produkt der SQS AG entsprechend in der im Gutachten genannten Form verwen-

det werden. In der Produktbeschreibung des Herstellers wird noch die Bezeichnung SAP HR verwendet. Das ist für die datenschutzrechtliche Prüfung jedoch nicht entscheidend gewesen, da die Umbenennung von SAP HR in SAP HCM keinerlei Relevanz auf die inhaltliche Prüfung hatte.

8 Die SQS-Teststuite für SAP HCM wird vom Hersteller zwar als „Beratungs*produkt*“ bezeichnet. Es handelt sich jedoch um ein Verfahren in Form einer Beratung bzw. um standardisierter Methoden, die mittels Softwareunterstützung durch die SQS AG bei öffentlichen oder nichtöffentlichen Stellen eingesetzt werden, um Tests mit automatisch generierten Testdaten durchzuführen, um Test an Produktivsystemen mit Echtdaten oder Test in Test- oder Entwicklungssystemen mit Echtdaten zu vermeiden.

D. Zweck und Einsatzbereich des Begutachtungsgegenstandes

9 Diesbezüglich wird auf das Erstgutachten verwiesen.

E. Tools, die zur Herstellung des IT-Produktes verwendet wurden

10 Das Verfahren basiert im Wesentlichen darauf, dass über die SAP-Funktionalität „eCATT“ Skripte generiert werden, mit denen Tests bzw. Testfälle automatisiert erzeugt werden können. Z.B. wird so die Eingabe von Daten in SAP simuliert, Prozesse (z.B. Abrechnung Lohn/Gehalt) initiiert etc. Die Erzeugung der eCATTs ist zwar abhängig von der jeweiligen SAP-Installation und -Konfiguration der verantwortlichen Stelle, sie erfolgt aber nach einer systematischen Methode. Die Durchführung der Tests erfolgt dann automatisiert.

11 Die Tests können innerhalb von SAP mit „Bordmitteln“ erfolgen (SAP Testworkbench oder SAP Solution Manager) oder durch Nutzung der Software SQS-Test/Professional Version 8, mit der eine höhere Transparenz und übersichtlichere Ergebnisprotokolle erreicht werden können. Die Software SQS-Test/Professional ist nicht Gegenstand der Zertifizierung. Die Gutachter haben die Software jedoch in Köln beim Hersteller in Augenschein nehmen können. Es bestehen keine Bedenken gegen einen datenschutzkonformen Einsatz der Software. Die Software muss zudem stets individuell an die IT-Umgebung/SAP-Umgebung der verantwortlichen Stelle angepasst werden. Die Anpassung erfolgt durch den Hersteller.

F. Primärdaten

12 Primärdaten, die datenschutzrelevant wären, fallen beim Einsatz des Verfahrens nicht an. Die Primärdaten wären hier die Testdaten in SAP HCM. Diese werden jedoch automatisch generiert und enthalten sog. Dummy-Daten (z.B. „Anton Tester“, „Max Mustermann“, „Anja Test“ etc.), die keinen Bezug zu konkreten Personen haben.

G. Sekundärdaten

13 Bei dem Einsatz des Verfahrens SQS-Testsuite für SAP HR fallen - abhängig von der jeweiligen Konfiguration des SAP-Systems der verantwortlichen Stelle - Sekundärdaten an. Dabei handelt es sich, worauf in der Produktbeschreibung des Herstellers richtig hingewiesen wird, um Daten, die sich aus der eCATT-Protokollierung in SAP ergeben. Dort kann ggf. protokolliert, werden, *welcher Benutzer, zu welchem Zeitpunkt, mit welchen Testdaten, welche Tests* (SAP-Transaktionen) durchgeführt hat. Ob und in welchem Umfang diese Daten gespeichert werden, obliegt der jeweiligen verantwortlichen Stelle.

14 Die SQS AG wirkt beim Einsatz des Verfahrens darauf hin, dass die Usernamen für Tester so gewählt werden, dass nicht schon aus dem Usernamen ein unmittelbarer Personenbezug für Dritte herstellbar ist (z.B. statt Benutzername=Nachname, Benutzername=TestuserX).

15 Bei der Nutzung der Software SQS-Test/Professional können ebenfalls Sekundärdaten in Testprotokollen in gleicher Weise anfallen. Die Software kann jedoch sehr individuell und nach Kundenwünschen konfiguriert werden. So kann die automatsierte Löschung von Protokollen nach Tagen eingestellt werden etc. Dies wird jedoch nach Maßgabe des Kunden und seinen Maßstäben an eine Vorabkontrolle und nach Vorgaben der Revision individuell konfiguriert.

H. Datenschutzrechtliche Bewertung

16 In dem Verfahren selbst steht die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nicht im Vordergrund. Es fallen lediglich Daten im Rahmen der Dokumentation und Kontrolle von Tests beiläufig in Form von Sekundärdaten an.

17 Das Verfahren selbst kann als Datenschutz-Verfahren bezeichnet werden. Es ist ein ideales Mittel, um die gesetzlichen Vorgaben an eine Vorabkontrolle einzuhalten.

18 Beim Einsatz von SAP HCM werden auch sog. sensitive Daten verarbeitet. Vor dem Einspielen neuer SAP-Versionen (Upgrades, Patches etc.) oder Vornahme neuer Konfigurationen muss nach § 9 LDSG-SH (bzw. § 4d Abs. 5 BDSG) eine Vorabkontrolle stattfinden. Bei einer Vorabkontrolle muss sowohl die Rechtmäßigkeit der Datenverarbeitung als auch die Ordnungsmäßigkeit der Datenverarbeitung (Datensicherheit) festgestellt werden. Die Vorabkontrolle obliegt der verantwortlichen Stelle (dort: dem Datenschutzbeauftragten).

19 Während die Prüfung der Rechtmäßigkeit der Datenverarbeitung nicht Gegenstand des Verfahrens ist, ist das Verfahren jedoch geeignet, um die Prüfung der Ordnungsmäßigkeit der Datenverarbeitung zu unterstützen. Die Prüfung der Ordnungsmäßigkeit der Datenverarbeitung setzt bei öffentlichen Stellen des Landes Schleswig-Holstein voraus (für Vorabkontrollen nach dem BDSG gelten jedoch ähnliche Maßstäbe), dass die in automatisierten Verfahren eingesetzten Programme *vor* der Aufnahme der Verarbeitung personenbezogener Daten zu testen sind (§ 7 Abs. 1 Satz 1 DSVO). Ferner sind die Testmaßnahmen und Ergebnisse sowie die bei den Tests eingesetzten informationstechnischen Geräte und Programme zu protokollieren (§ 7 Abs. 1 Satz 2 DSVO).

20 Diese Anforderungen setzt das Verfahren vollständig um. Die Bewertung des Verfahrens kann bezüglich der Umsetzung der Anforderung an die Durchführung einer Vorabkontrolle als vorbildlich bewertet werden.

I. Zusammenfassung

21 Das Verfahren SQS-Testsuite für SAP HCM genügt den datenschutzrechtlichen Anforderungen in vollem Umfang. Das Verfahren gewährleistet die Einhaltung eines wesentlichen Bestandteils des Datenschutzes bzw. der Datensicherheit: nämlich das umfassende Testen von automatisierten Verfahren, mit denen (sensitive) personenbezogene Daten verarbeitet werden sollen, mit nicht-personenbezogenen Testdaten im Vorwege.

22 Das Anfallen von Sekundärdaten ist dabei datenschutzrechtlich sogar erwünscht, da anderenfalls die Vorgaben an die Dokumentation der Vorabkontrolle i.S.d. § 7 Abs. 1 DSVO nicht eingehalten werden könnten.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Flensburg, den 11.04.2008

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum
für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (rechtlich)

Kellinghusen, den 11.04.2008

Andreas Bethke
Dipl. Informatiker (FH)
Beim Unabhängigen Landeszentrum
für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (technisch)