Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für das IT-Produkt BKMS® System

im Auftrag der Business Keeper AG

datenschutz cert GmbH

18. September 2013

Inhaltsverzeichnis

1. Über dieses Kurzgutachten

Mit diesem Kurzgutachten wird die Auditierung des IT-Produkts „Business Keeper Monitoring System (BKMS® System)“ in der Version 2.7.3 der Business Keeper AG zusammengefasst, mit welcher die Prüfstelle der datenschutz cert GmbH beauftragt wurde.

Ziel der rechtlichen und technischen Auditierung ist die Erlangung des Datenschutz-Gütesiegels gemäß der Landesverordnung über ein Datenschutzaudit (DSAVO) in Schleswig-Holstein[1], welches durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (kurz ULD) vergeben wird. Hervorzuheben ist, dass das BKMS® System bereits im Juni 2013 nach Auditierung durch Experten der datenschutz cert GmbH seitens des ULD mit dem Datenschutz-Gütesiegel „EuroPriSe“ (European Privacy Seal)[2] ausgezeichnet wurde.

2. Zeitraum der Prüfung

Die Begutachtung des BKMS® System erstreckte sich auf den Zeitraum von 27.11.2012 bis 03.06.2013 und beinhaltete neben der konzeptionellen Analyse der zur Verfügung gestellten Unterlagen die Durchführung von Plausibilitätstests.

3. Antragstellerin

Antragstellerin dieses Gutachtens ist die

Business Keeper AG,
Bayreuther Straße 35,
10789 Berlin

als Hersteller und Anbieter. Ansprechpartner ist Herr Kenan Tur.

4. Sachverständiger/Prüfstelle

Sachverständige dieser Auditierung ist die Prüfstelle für Recht und Technik

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Dr. Irene Karper (Recht).

Ansprechpartner für diese Begutachtung sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

---

[1] Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung - DSAVO) v. 18.11.2009, *GVOBl.* Schl.-H. *2008, S. 562ff. / GVOBl.* Schl.-H. *2009, S. 742ff.* Das Datenschutz-Gütesiegel des ULD ist in der Bundesrepublik Deutschland bundesweit anerkannt.

[2] EuroPriSe ist ein international anerkannter Standard für ein Datenschutzgütesiegel. Mit dem Siegel wird die Konformität von IT-Produkten und IT-basierenden Services zu den Europäischen Datenschutz-Vorgaben bestätigt. Es wird von Zertifizierungsstelle in teilnehmenden Staaten der Europäischen Union vergeben. Zertifizierungsstelle in der Bundesrepublik Deutschland ist das ULD. Weitere Informationen sind abrufbar unter https://www.european-privacy-seal.eu/ (diese und alle nachfolgenden Webseitenverweise waren mit Stand zum September 2013 gültig).

5. Kurzbezeichnung des IT-Produkts

Auditiert wurde das IT-Produkt BKMS® System (Business Keeper Monitoring System) in der Version 2.7.3. Dabei wurde der Funktionsstand des Verschlüsselungsmoduls mit der SHA256-Prüfsumme

bd4570f7bb1e2171c246dac7a137e395988c2bde55c85e16b8e986e091e83495

zugrunde gelegt.

BKMS® System wird von der Business Keeper AG als Software as a Service (SaaS) im Auftrag für den Anwender entwickelt, gepflegt und in einem Rechenzentrum in Deutschland betrieben. Dieser IT-Service mit Stand zum Mai 2013 wurde ebenfalls in die Auditierung einbezogen.

6. Beschreibung des IT-Produkts

BKMS® System ist eine webbasierende Anwendung, die in den Konstellationen

- BKMS-Z (Hinweise laufen in einer zentralen Stelle auf und werden von dort zugewiesen)
- BKMS-D (Hinweise laufen direkt beim jeweiligen Hinweisbearbeiter auf)
- BKMS-O (In die Hinweisbearbeitung werden externe Personen, z.B. Ombudsleute, eingebunden)

zur Verfügung gestellt wird. Zum Auditgegenstand gehören ein Produktivsystem mit einem Loadbalancer, zwei Anwendungsservern und einem Datenbankserver sowie ein Entwicklungs- und Testsystem.

Nicht zum Auditgegenstand gehören spezielle Konfigurationen durch den Anwender, insbesondere die eines externen Übersetzers, von individuellen Auswertungsreports sowie nicht-standardisierten Melde-Themen, Begrüßungstexten oder Einwilligungserklärungen. Ebenfalls nicht Auditgegenstand sind andere Serviceleistungen der Business Keeper AG, der Vertriebsprozess sowie die Einrichtungsumgebung beim Anwender oder beim Hinweisgeber.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Keine.

8. Zweck und Einsatzbereich

BKMS® System ermöglicht einen Dialog zwischen Hinweisgebern und Hinweisbearbeitern, um Missstände, Gefahren oder Risiken melden zu können. Es wird als „Whistleblowing"-System zur Unterstützung des Wertemanagements, der Compliance oder der Revision eingesetzt. Anwender des BKMS® System sind Unternehmen, Organisationen oder öffentliche Stellen. Hinweisbearbeiter sind in der Regel Mitarbeiter des Anwenders, wie Compliance-Beauftragte oder vom Anwender freigegebene externe Experten, wie z.B. Ombudsleute. Hinweisgeber von Missständen, Gefahren oder Risiken sind typischer Weise Bürger, Mitarbeiter oder Vertragspartner.

Der Zugriff auf das BKMS® System erfolgt über eine https-Schnittstelle. Die Anmeldemaske für Hinweisbearbeiter ist unter https://www.business-keeper.com/kundenlogin.html erreichbar (September 2013). Üblicher Weise verlinken Anwender den Zugang für Hinweisgeber zum BKMS® System auf ihren eigenen Homepages.

Hinweisabgabe

Der Hinweisgeber kann in einem Webformular eine Meldung abgeben oder einen Postkasten anlegen, über welchen ein Dialog zum Hinweisbearbeiter erfolgen kann.

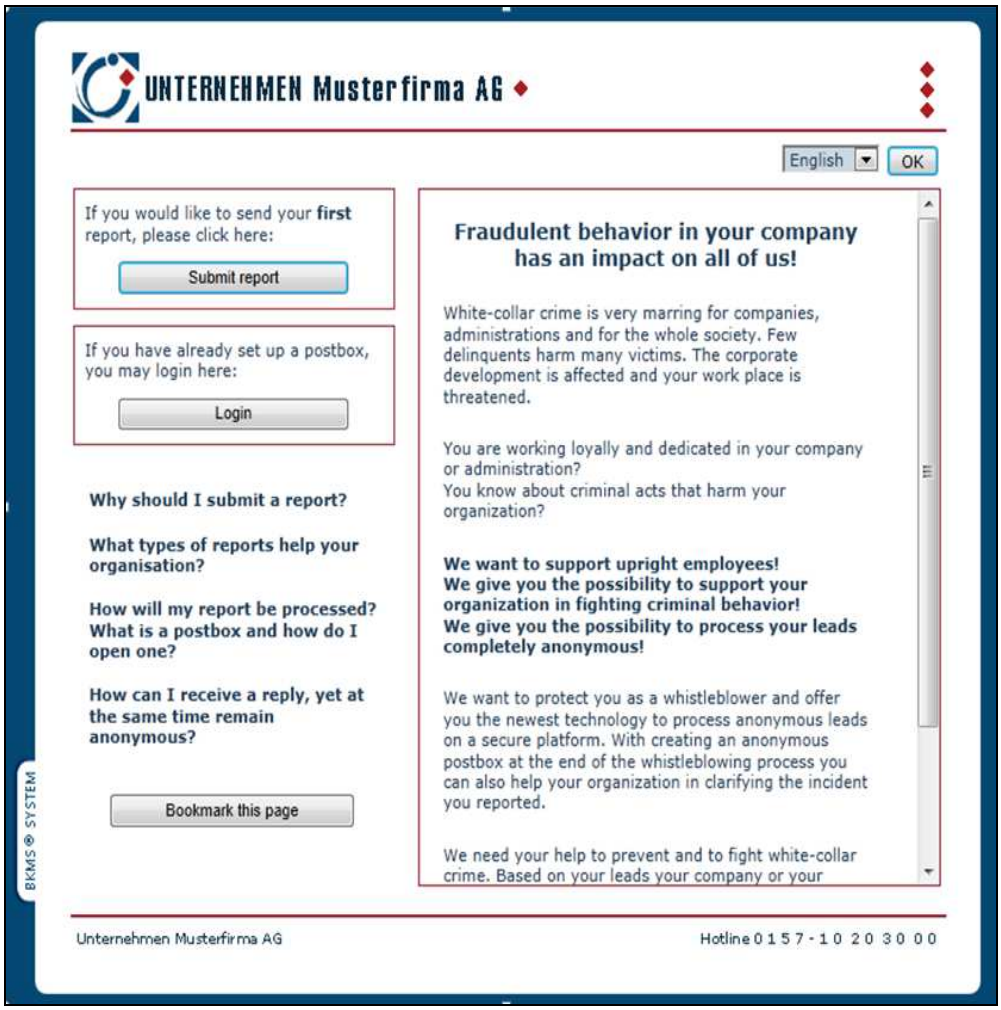

Abbildung 1: Ausschnitt aus der Anmeldemaske zum BKMS® System

Das BKMS® System präferiert eine personenbeziehbare Nutzung, ermöglicht jedoch auch eine anonyme Hinweisabgabe. Seitens der Business Keeper AG werden Hinweisgeber im vorgegebenen Standard-Webformular sowie Anwender in einem Merkblatt zum Datenschutz sowie bei Systemeinrichtung und Schulungen ausdrücklich aufgefordert, anonymisierte Meldungen nicht zu bevorzugen.

Im Rahmen der Hinweisabgabe erhält der Hinweisgeber Informationen zur Nutzung. Je nach Anforderung können auch besondere Datenschutzerklärungen oder

Einwilligungen (z.B. bei Weitergabe an Standorte außerhalb der EU) eingebunden werden.

Der Hinweisgeber wird dann auf bestimmte Melde-Themen geleitet.

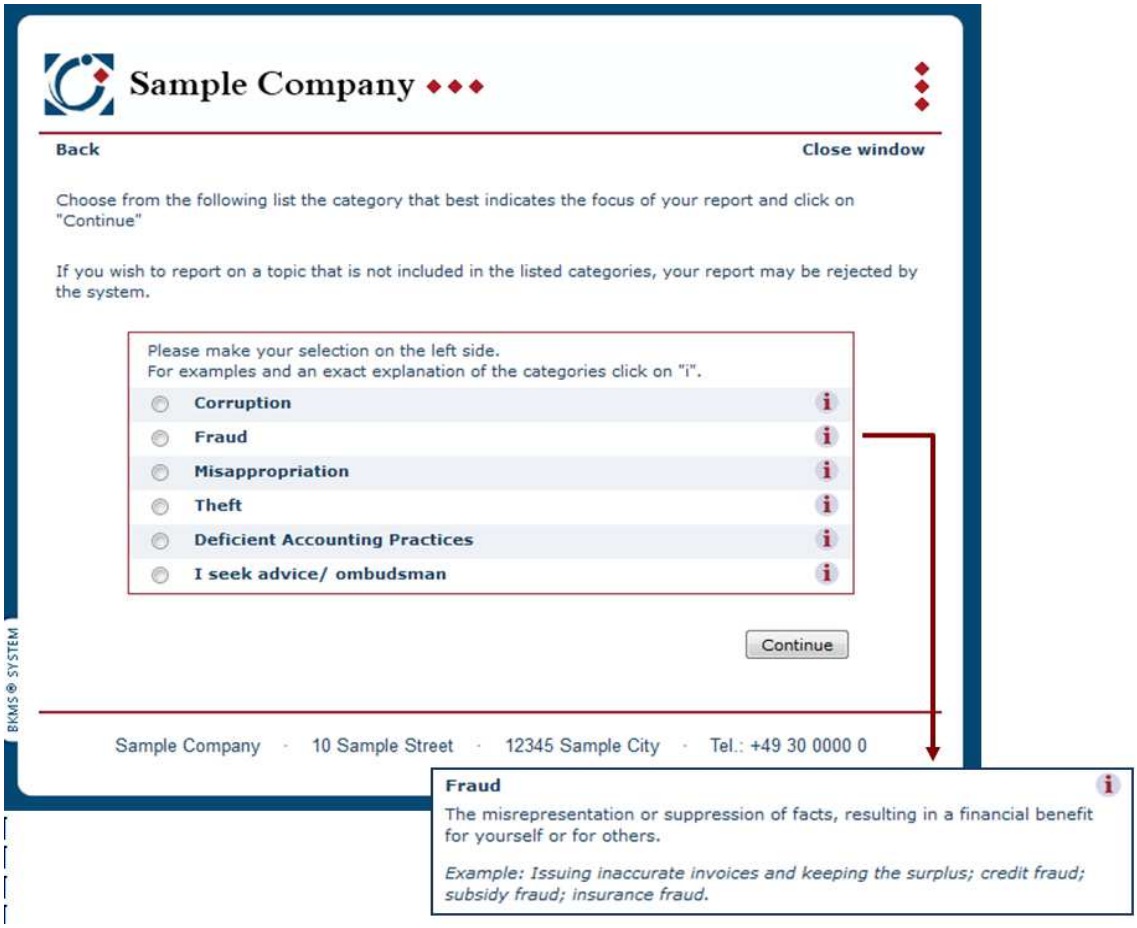

Abbildung 2: Beispiel für Melde-Themen

Die Definition der Melde-Themen erfolgt durch den Anwender anhand der für ihn geltenden Gesetze oder Regelungen. Die in der Standardausführung vorgegebenen Themen beziehen sich auf Straftaten, nicht aber auf Verstöße gegen Ethik- und Verhaltensregeln, da hier in der Regel das schutzwürdige Interesse der Betroffenen gegen eine Datenerfassung spricht. Der Anwender kann gleichwohl derartige Melde-Themen konfigurieren. Er wird durch ein Merkblatt zum Datenschutz, durch ein Handbuch für Accountspezifikationen sowie in Schulungen auf die rechtskonforme Systemeinrichtung sensibilisiert.

Anschließend kann der Hinweisgeber seine Angaben konkretisieren und z.B. Dateien hochladen.

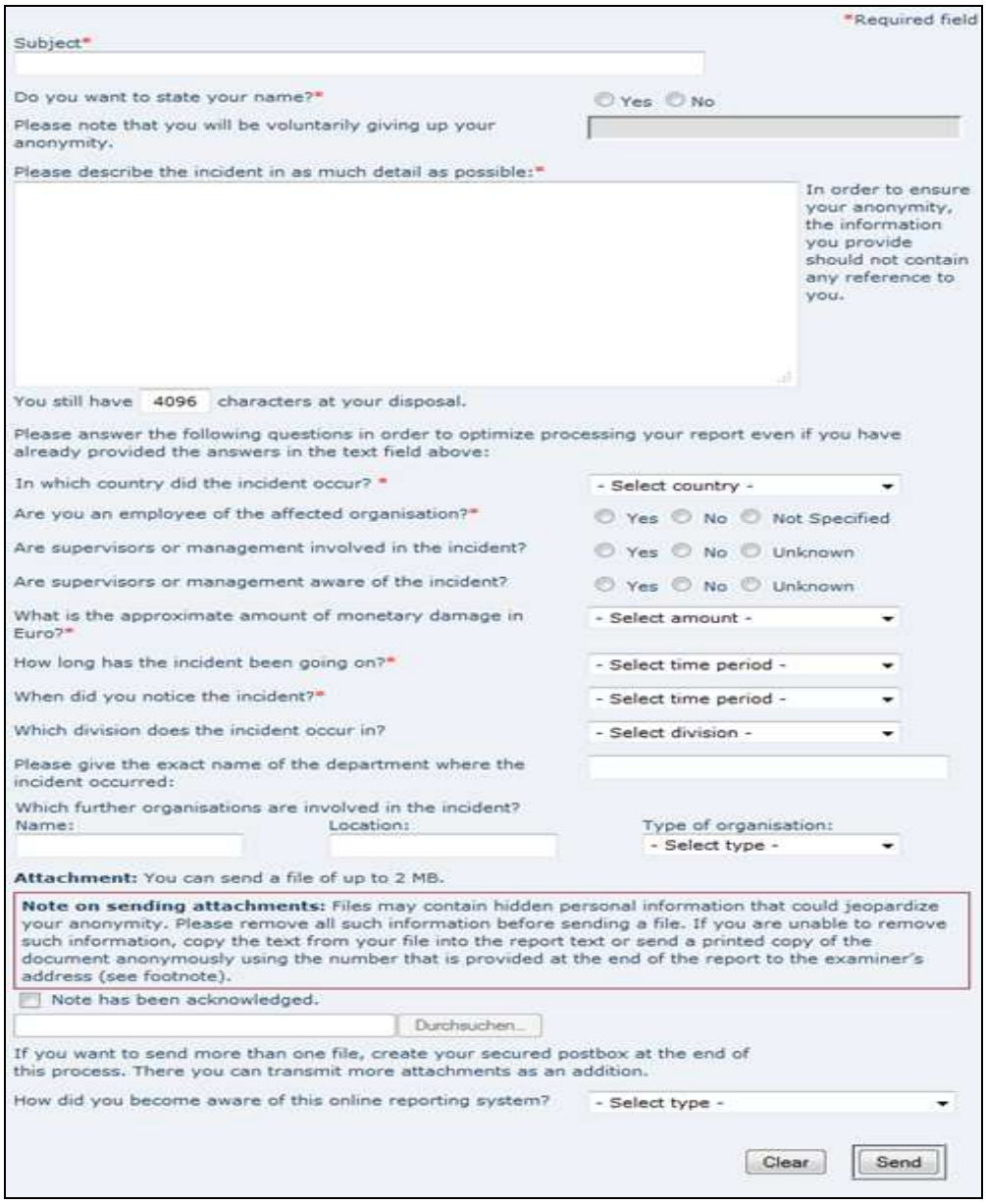

Abbildung 3 Datenerfassungsmaske für Hinweisabgabe

Anwender können für die Formulareingabe Schlüsselwörter definieren, die als unzulässig ausgefiltert werden (z.B. Beleidigungen). Ist ein solcher Begriff enthalten, wird die Meldung nicht angenommen und der Hinweisgeber darüber informiert.

Nach Abschicken der Meldung erhält der Hinweisgeber eine Referenznummer, anhand derer die Meldung bearbeitet wird. Die Meldung kann ausgedruckt werden.

Postkasten

Der Hinweisgeber kann einen Postkasten einrichten, um so ggf. in den Dialog mit dem Hinweisbearbeiter treten zu können. Dabei wird er im Formularfeld darauf hingewiesen, dass er ein Pseudonym als Benutzername wählen kann. Das Passwort wird als Hash gespeichert. Bei Verlust der Zugangsdaten können diese weder

administrativ noch systemseitig wiederhergestellt werden. Der Postkasten wird verschlüsselt und eine Postkasten-ID angelegt. Über den Postkasten erhält der Hinweisgeber Informationen zum Bearbeitungsstand und kann Ergänzungen senden. Inhalte der Meldungen sind für 42 Tage zum Lesen und Drucken vorhanden.

Hinweisbearbeitung

Hinweisbearbeiter müssen sich am System mit Benutzername und Passwort anmelden. Das Passwort ist als Hashwert gespeichert. Mit Zugriff werden Benutzer-ID, eine Benutzer-Zugriffsrechte-ID und eine Anwender-ID in der Datenbank gespeichert. Der Hinweisbearbeiter erhält nach Login eine Statusübersicht und kann Meldungen z.B. sortieren oder auf Wiedervorlage legen.

Zur Accountaktivierung und -nutzung wird als zusätzlicher Sicherheitsaspekt bei der Zuordnung von Berechtigungen eine „DatenPIN“ benötigt, die verschlüsselt in der Datenbank hinterlegt ist. Bei Verlust kann die Korrespondenz nicht wiederhergestellt werden. Nach Eingabe der DatenPIN kann der Hinweisbearbeiter Meldungen bearbeiten, als Administrator Einstellungen vornehmen sowie als Systemadministrator Zugänge verwalten.

Frühwarnsystem

BKMS® System enthält ein Frühwarnsystem, welches bei bestimmten Schlüsselbegriffen in einer Meldung eine SMS, E-Mail oder ein Fax an ausgewählte Personen schickt. Das Frühwarnsystem soll die Reaktionszeit bei spezifischen Risiken verringern. Hierfür werden Anwender-ID und E-Mail-Adresse bzw. Telefon- oder Faxnummer der autorisierten Stelle in der Datenbank gespeichert.

Datenschutzfunktion

Bei der Datenschutzfunktion können Meldungsinhalte unkenntlich gemacht werden, indem ein Personenbezug geschwärzt bzw. entfernt wird und dann für die weitere Bearbeitung nicht mehr sichtbar ist.

Übersetzungsfunktionen

Nicht vom Standardumfang von BKMS® System umfasst ist die optional konfigurierbare Rolle eines externen Übersetzers, für den Meldungen zur Übersetzung freigegeben werden können. Diese Rolle ist als Auftragsdatenverarbeitung zu qualifizieren.

Auswertungsmöglichkeiten

BKMS® System bietet Datenauswertungen, wie z.B. Logreports zur Auswertung der Systemzugriffe oder Standardreports mit nicht-personenbeziehbaren Auswertungen von Hinweisen. Auf Wunsch des Anwenders können auch individuelle Reports konfiguriert werden, was aber nicht vom Standardumfang umfasst ist.

Verschlüsselung der Daten

Zur Verschlüsselung der Meldungen wird ein asymmetrisches Kryptosystem (Public-Key-Verfahren) eingesetzt. Das Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel, wird durch eine Passphrase ergänzt, welche verteilt auf die Business Keeper AG sowie auf den Anwender aufbewahrt wird. Auf diese Weise wird

sichergestellt, dass die Business Keeper AG keinen Zugriff auf Meldungen hat. Eine Meldung kann nur unter Eingabe der DatenPIN entschlüsselt werden.

Unterschiedliche Datenbanken pro Anwender sowie die Verschlüsselung setzen die Datentrennung um.

Archivierung und Löschung

Meldungen können durch Bearbeiter gelöscht oder archiviert werden. Bei Löschung eines Benutzers werden diesem alle Rechte entzogen. Name, Vorname und Alias/Kürzel bleiben erhalten, um Doubletten zu verhindern und Aktivitäten im Log revisionssicher zuordnen zu können.

Aktivitätslogs mit dem Bearbeiter-Alias werden in der Standardkonfiguration von BKMS® System für 3 Jahren aufbewahrt, um längeren Revisionen, Gerichtsverfahren und Verjährungsfristen entsprechen zu können. Auf Wunsch des Anwenders können kürzere Löschfristen eingerichtet werden.

Mit Löschung eines Anwender-Accounts werden sämtliche Daten unmittelbar nach Vertragsschluss seitens der Business Keeper AG gelöscht.

Administration von BKMS

Der Administrator des Anwenders verwaltet die Accounteinstellungen und kann Textbausteine bearbeiten. Der vom Anwender definierte Systemadministrator erteilt oder entzieht Zugangsberechtigungen und kann Hinweisbearbeiter einrichten, ändern oder löschen. Dabei hat er keinen Zugriff auf Meldungsinhalte. Der Systemadministrator kann Rechte in BKMS® System sehr detailliert abstufen.

Über eine SSH-Schnittstelle greift die Business Keeper AG auf die Server des BKMS® System zu Wartungs- und Backupzwecken zu.

Verantwortliche Stelle und Auftragsdatenverarbeiter

Der Anwender von BKMS® System ist als datenschutzrechtlich verantwortliche Stelle einzuordnen. Werden im Rahmen von BKMS-O externe Stellen, wie z.B. Ombudsleute, in den Workflow eingebunden, handelt es sich in der Regel um eigenverantwortliche Stellen der Datenverarbeitung, sofern diese in größerem Umfang über die Bearbeitung oder Bewertung eines Hinweises (mit-)entscheiden. Erhalten sie Daten mittels BKMS® System, handelt es sich um eine Datenübermittlung.

Die Business Keeper AG ist Auftragsdatenverarbeiter. Hervorzuheben ist, dass das Unternehmen im Rahmen des SaaS nur auf verschlüsselte Daten zugreifen könnte. Dies gilt auch für die Telekom Deutschland GmbH, die im Unterauftrag das Rechenzentrum in Deutschland betreibt.

9. Modellierung des Datenflusses

Der Datenfluss lässt sich grafisch wie folgt darstellen:

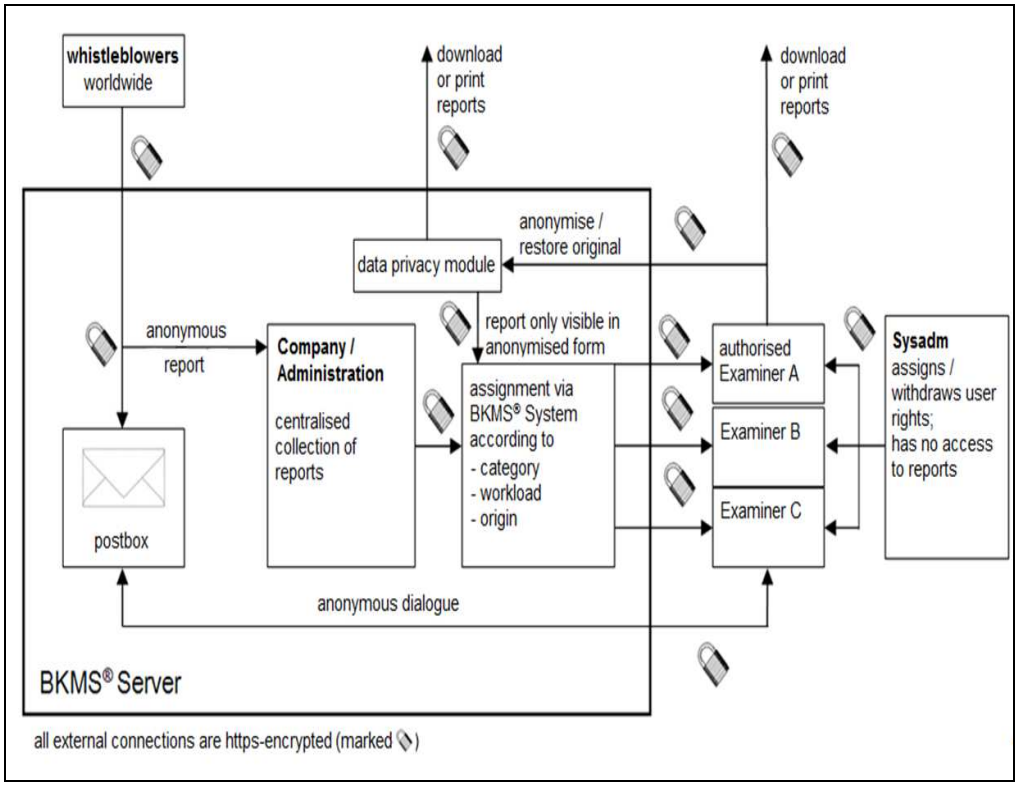

Abbildung 1: Datenerfassungsmaske für Hinweisabgabe

10. Version des der Prüfung zugrunde gelegten Anforderungskatalogs

Version 1.2

11. Zusammenfassung der Prüfergebnisse

Anwendbares Recht und Umsetzung

Die Einrichtung von Hinweissystemen (Whistleblowing-Systemen) erfolgt zumeist aufgrund der für Anwender geltenden Sonderbestimmungen. An erster Stelle zu nennen ist hier der Sarbanes-Oxley-Act (SOX)[3], der börsennotierten Unternehmen in den USA – und mittelbar auch deren Unternehmensbestandteilen in der Bundesrepublik Deutschland - interne Kontrollmaßnahmen vorgibt. Daneben gibt es zahlreiche Bestimmungen zu Meldemöglichkeiten oder -pflichten bei Regelverstößen, wie etwa die OECD Anti-Korruptionskonvention[4] oder § 11 Geldwäschegesetz, § 10 Wertpapierhandelsgesetz, § 16 Abs. 1 Arbeitsschutzgesetz sowie Remonstrationspflichten im Beamtenrecht. Denkbar sind ferner individuelle oder kollektive Vereinbarungen über Hinweise bei Regelverstößen.

[3] Abrufbar unter http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR: .

[4] Convention on Combating Bribery of Foreign Public Officials in International Business Transactions vom 21.11.1997, abrufbar unter http://www.oecd.org/investment/briberyininternationalbusiness/anti-briberyconvention/38028044.pdf i.V.m. den Good Corporate Governance Principles der OECD, abrufbar unter http://www.oecd.org/daf/corporateaffairs/corporategovernanceprinciples/31557724.pdf .

Dabei ist hervorzuheben, dass ausländische bzw. internationale Regelungen, wie der SOX, keine datenschutzrechtlichem Grundlagen der Datenverarbeitung und Datenübermittlung im Sinne nationaler Datenschutzbestimmungen darstellen[5].

Rechtsgrundlage der Datenverarbeitung und Datenübermittlung in Hinweissystemen ist vielmehr § 28 Abs. 1 S. 1. Nr. 2 Bundesdatenschutzgesetz (BDSG)[6] als allgemeine Regelung, sowie als *lex specialis* für den Bereich der Beschäftigtendatenverarbeitung § 32 Abs. 1 S. 2 BDSG. Rechtsgrundlage kann zudem eine Einwilligungserklärung der Betroffenen sein, sofern diese die Voraussetzungen der §§ 4, 4a BDSG erfüllt. Für die Anwendung durch öffentliche Stellen gilt hingegen das jeweilige Landesrecht, so dass für diese Auditierung §§ 11ff. Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H)[7] und die Datenschutzverordnung (DSVO) Schleswig-Holstein[8] heranzuziehen sind.

Zudem sind die Auslegungshilfen der Artikel-29-Datenschutzgruppe der Europäischen Union (EU), die Rechtsprechung der deutschen und Europäischen Gerichtshöfe sowie ggf. nationale Vorgaben oder Auslegungshilfen der Datenschutzaufsichtsbehörden zu beachten. Diesbezüglich ist Working Paper No. 117 der Artikel-29-Datenschutzgruppe („*Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*")[9] zu nennen, sowie Richtlinien für die Implementierung von Whistleblowing-Systemen der französischen Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL)[10] und der Arbeitsbericht der deutschen Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz" des Düsseldorfer Kreises zum Thema „*Whistleblowing – Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz*"[11].

Hervorzuheben ist, dass BKMS® System die Einhaltung der jeweiligen Rechtsgrundlagen nicht garantieren kann, da dies ausschließlich im Verantwortungsbereich des Anwenders liegt. Allerdings wird der Anwender durch das Merkblatt zum Datenschutz aufgefordert, die Rechtskonformität zu überprüfen, so dass eine angemessene Sensibilisierung erfolgt.

Hinweisgebersysteme sind i.S.d. § 28 BDSG und §§ 11ff. LDSG S-H zulässig, wenn sie vertraglichen Zwecken dienen, auf einer ausdrücklichen Einwilligung beruhen oder im berechtigten Interesse einer Organisation oder eines Unternehmens erfolgen, ohne das schutzwürdige Interessen der Betroffenen dem entgegenstehen. Hierbei ist zu berücksichtigen, dass gemeldete Daten personenbezogen oder zumindest

---

[5] Dies ist die überwiegende Rechtsauffassung, vgl. auch Working Paper No. 117 der Art-29-Datenschutzgruppe.
[6] 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).
[7] Landesdatenschutzgesetz - LDSG - Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen v. 09.02.2000, zuletzt geändert durch Artikel 1 des Gesetzes zur Schaffung einer gesetzlichen Grundlage für die Datenschutzordnung des Landtags v. 6. April 2013, GVOBl. Schl.-H. 25/2013, S. 125).
[8] Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten v. 09. 1 2008 , GVOBl Schl.-H. 2008, S. 841ff.
[9] Abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
[10] Vom 10.11.2005, abrufbar unter http://www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf . Die Richtlinie bildete u.a. die Grundlage für das Working Paper No. 117 der Art-29-Datenschutzgruppe.
[11] Abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=246.

personenbeziehbar sind, soweit sie Rückschlüsse auf eine natürliche Person zulassen. Sofern Meldungen z.B. religiöse Hintergründe oder sexuelles Verhalten thematisieren, werden auch besondere personenbezogene Daten mittels BKMS® System verarbeitet. Letzteres erfordert eine informierte, freiwillige und ausdrückliche Einwilligung aller betroffenen Personen. Im Beschäftigungsverhältnis scheidet eine Einwilligung dabei regelmäßig aus, da sie mangels Freiwilligkeit nicht wirksam erteilt werden kann[12]. Das Einwilligungserfordernis kann allerdings mit Hilfe von BKMS® System auch entfallen, sofern die Daten des Betroffenen mittels BKMS® System pseudonymisiert oder anonymisiert werden.

Meldungen dürfen Verstöße in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Korruption, sowie Banken- und Finanzkriminalität oder Verstöße gegen Menschenrechte und Umweltbelange betreffen (sogenannte „Harte Faktoren"). Grundsätzlich nicht zulässig sind hingegen Meldungen über Verstöße gegen „weiche Faktoren", wie z.B. Ethik-, oder Verhaltensregelungen; diese können nur gerechtfertigt sein, wenn keine schutzwürdigen Interessen der Betroffenen dem entgegenstehen. Das BKMS® System setzt diese Unterscheidung durch Basis-Themenlisten und Filterfunktionen für Meldungen angemessen um.

Indem mittels BKMS® System Missstände, Gefahren oder Risiken für die Allgemeinheit abgewendet werden können, erfolgt dies zudem grundsätzlich im öffentlichen Interesse, so dass auch ein Einsatz durch öffentliche Stellen grundsätzlich zulässig ist.

Für eine Weitergabe von Daten über BKMS® System an externe Stellen bzw. an einen Dritten ist der Anwender verantwortlich. Dies gilt auch bei einer Datenübermittlung in Staaten außerhalb der EU und des Europäischen Wirtschaftsraumes, wobei der Anwender hier neben der Zulässigkeit der Datenübermittlung auch ein angemessenes Schutzniveau im Empfängerstaat nachweisen muss. Der Anwender wird hierauf im Datenschutzhinweisblatt auf die für ihn ggf. geltenden Bestimmungen, die Vorabkontroll- und sowie Informationspflichten sensibilisiert. Zudem können Rollen und Berechtigungen im BKMS® System so abgestuft werden, dass eine Übermittlung nur im restriktiven Umfang möglich gemacht wird.

Sowohl bei der Hinweisabgabe über Online-Formulare als auch bei der Frühwarnfunktion per SMS und E-Mail ist die Vertraulichkeit der Kommunikation sichergestellt. Webseiten sind per https verschlüsselt und damit vor unbefugtem Auslesen der Kommunikation während der Datenübertragung angemessen geschützt. Loginfunktionen erfordern ein sicheres Passwort. Die Verschlüsselung der Daten sichert die Vertraulichkeit. Auch das Setzen eines Cookies ist hier erforderlich und damit rechtmäßig, da sie die vom Hinweisgeber gewünschte Nutzung von BKMS® System ermöglichen.

---

[12] Siehe hierzu Abschnitt D. 4 des Arbeitsberichts der deutschen Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz" des Düsseldorfer Kreises zum Thema „Whistleblowing – Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz.

Auch die Verarbeitung personenbeziehbarer Protokolldaten über Aktivität und Zeitpunkt ist zulässig, da sie für die Kontrolle der berechtigten Nutzung– und damit als technisch-organisatorische Maßnahmen des Datenschutzes – erforderlich ist.

Datenvermeidung und Datensparsamkeit

BKMS® System ermöglicht eine Anonymisierung anhand der Datenschutzfunktion sowie anonymisierte statistische Auswertungen. Hierüber können zudem personenbezogene oder –beziehbare Daten gelöscht oder auf das Notwendigste reduziert werden. Sekundärdaten, wie z.B. Logfiles, werden nur für kurze Zeit aufbewahrt und automatisch gelöscht. Berechtigungen und der Zugang zu Daten können ebenfalls auf ein notwendiges Maß reduziert werden. Anwender werden durch das Merkblatt zum Datenschutz auf die Umsetzung von Datensparsamkeit und Datenvermeidung hingewiesen.

Datensicherheit

Die Server werden in einem Rechenzentrum mit hohen Zugangskontrollen und starker Verfügbarkeit geführt. Datenübertragungen werden über SSL abgesichert. Ein angemessenes Backupkonzept sowie ein Notfallplan unterstützen die Verfügbarkeit. Allerdings ist dieser Notfallplan noch um Maßnahmen zum Virenschutz zu ergänzen, was zum Zeitpunkt der Auditierung noch nicht vollständig dokumentiert war. Dies gilt auch für eine Dienstanweisung zum Umgang mit Accountdaten von ausgeschiedenen Mitarbeitern. Die Business Keeper AG hat allerdings eine Umsetzung bis zum nächsten Monitoring im Rahmen des EuroPriSe-Verfahrens angekündigt.

Die Business Keeper AG hält für Anwender ein Vertragskonvolut zur Verfügung, welches die Anforderungen des § 11 BDSG und § 17 LDSG S-H entspricht. Auch der Unterauftrag zwischen der Business Keeper AG und der Telekom Deutschland GmbH erfüllt diese Anforderungen.

Umsetzung von Betroffenenrechten

Die Business Keeper AG hat zahlreiche Informationen und Datenschutzhinweise auf den Webseiten sowie Anwendungsdokumentationen veröffentlicht, welche es dem Anwender bzw. Hinweisgeber ermöglichen, ganz im Sinne der informationellen Selbstbestimmung die Datenverarbeitung zu beeinflussen. Betroffenenrechte, wie z.B. Auskunftsersuchen oder Widerruf von Einwilligungen, können durch BKMS® System unterstützt werden durch schnellen Datenzugriff und Auswertungen.

12. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Die Vertraulichkeit der Daten wird bei BKMS® System durch ein Berechtigungskonzept optimal sichergestellt, welches die Vergabe sehr differenzierter Zugriffsrechte ermöglicht.

Service-Beschreibungen und Informationen zur Datenverarbeitung sind vorbildlich transparent und ermöglichen die Umsetzung der Betroffenenrechte in optimaler Weise.

Organisatorische und technische Maßnahmen gehen über die gesetzlichen Anforderungen hinaus.

Der Auftragnehmer sensibilisiert den Anwender in vorbildlicher Weise auf die Einhaltung des Datenschutzes, u.a. durch ein Datenschutzhinweisblatt.

Das Rechenzentrum, in welchem sich die Komponenten von BKMS® System befinden, weist ein hohes Maß an physikalischer Sicherheit aus.

13. Votum der Auditoren

Das BKMS® System erfüllt alle Anforderungen an den Datenschutz und die Datensicherheit in besonderer Weise. Die Auditoren empfehlen die Zertifizierung.

Bremen, 18. September 2013

Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH