

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

_____ im Auftrag der Business Keeper AG

_____ datenschutz cert GmbH

1. August 2015

Inhaltsverzeichnis

1.	Über dieses Kurzgutachten	3
2.	Zeitraum der Prüfung	3
3.	Antragstellerin	3
4.	Sachverständiger/Prüfstelle	3
5.	Kurzbezeichnung des IT-Produkts	4
6.	Beschreibung des IT-Produkts	4
7.	Tools, die zur Herstellung des Produkts verwendet wurden	5
8.	Zweck und Einsatzbereich	5
9.	Modellierung des Datenflusses	11
10.	Version des der Prüfung zugrunde gelegten Anforderungskatalogs	12
11.	Zusammenfassung der Prüfergebnisse	12
12.	Beschreibung, wie das IT-Produkt den Datenschutz fördert	15
13.	Votum der Auditoren	15

1. Über dieses Kurzgutachten

Mit diesem Kurzgutachten wird die Auditierung des IT-Produkts „Business Keeper Monitoring System (BKMS® System)“ in der Version 3.1 der Business Keeper AG zusammengefasst, mit welcher die Prüfstelle der datenschutz cert GmbH beauftragt wurde.

Ziel der rechtlichen und technischen Auditierung ist die erneute Erlangung des Datenschutz-Gütesiegels gemäß der gemäß der Datenschutzgütesiegelverordnung (DSGSVO)¹ in Schleswig-Holstein, welches durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (kurz ULD) vergeben wird.

Hervorzuheben ist, dass das BKMS® System bereits in der Vorversion nach Auditierung durch Experten der datenschutz cert GmbH seitens des ULD mit dem Datenschutz-Gütesiegel ausgezeichnet wurde. Zudem wurde das BKMS® System gemäß dem Gütesiegelstandard „EuroPriSe“ (European Privacy Seal)² seitens der Experten der datenschutz cert GmbH geprüft und durch die EuroPriSe GmbH zertifiziert.

2. Zeitraum der Prüfung

Die Begutachtung des BKMS® Systems erstreckte sich auf den Zeitraum vom 14.04.2015 bis zum 28.07.2015 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).

¹ Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) v. 30.11.2013, GVBl. Schl.-H. 2013, S.536ff. Sie ersetzt seit dem 01.01.2014 die Datenschutzauditverordnung.

² Das BKMS® System erhielt bereits in der Vorversion 2.7.3 erfolgreich das EuroPriSe-Zertifikat, vgl. <https://www.european-privacy-seal.eu/EPs-en/Business-Keeper> (Stand der Webseite ist August 2015). 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 die EuroPriSe GmbH. Weitere Informationen sind abrufbar unter <https://www.european-privacy-seal.eu/> (Stand August 2015).

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

5. Kurzbezeichnung des IT-Produkts

Auditiert wurde das IT-Produkt BKMS® System (Business Keeper Monitoring System) in der Version 3.1. Dabei wurde der Funktionsstand des Verschlüsselungsmoduls mit der SHA256-Prüfsumme

bd4570f7bb1e2171c246dac7a137e395988c2bde55c85e16b8e986e091e83495

zugrunde gelegt.

Das 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 April 2015 wurde ebenfalls in die Auditierung einbezogen.

6. Beschreibung des IT-Produkts

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

- BKMS® System als zentrale Lösung
- BKMS® System als dezentrale Lösung
- BKMS® System als Lösung mit externen Experten.

zur Verfügung gestellt wird.

Wird das BKMS® System als zentrale Lösung eingesetzt, laufen Hinweise in einer vom Anwender definierten zentralen Stelle beim Anwender auf und werden von dort an zuständige Hinweisbearbeiter zugewiesen.

Beim BKMS® System als dezentrale Lösung laufen die Hinweise direkt beim zuständigen Hinweisbearbeiter des Anwenders auf.

Das BKMS® System kann ferner auch externe Personen (z.B. Ombudsleute, Wirtschaftsprüfer) außerhalb des Anwenders in den Dialog einbinden.

Diese Varianten beschreiben lediglich Konstellationsmöglichkeiten beim Einsatz des BKMS® Systems. Es handelt sich um keine gesonderten Produkte oder separate IT-basierte Services. Auch weisen sie in technischer Hinsicht keine unterschiedlichen Soft- und Hardwarekomponenten aus. Sie werden nachfolgend gemeinsam als BKMS® System bezeichnet.

Zum Auditgegenstand gehören ein Produktivsystem mit einem Loadbalancer, vier 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

Das 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[®] Systems 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 sind typischer Weise Bürger, Mitarbeiter oder Vertragspartner.

Der Bearbeiterzugang des BKMS[®] Systems ist im Internet unter <https://client.bkms-system.net/bkwebanon/action/client/clientDisclaimer.do?language=ger> erreichbar³.

Dies ist die Anmeldemaske für Meldungsbearbeiter und Sysadmins..

Die jeweils aktuelle Version des BKMS[®] Systems wird dem Anwender durch ein Mouse-Over über das Logo verdeutlicht.

Üblicher Weise verlinken Anwender das System für Hinweisgeber auf ihren Homepages, wie z.B. die Bertelsmann SE & Co. KGaA unter <https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=berma45231&language=eng>.

Alternativ bietet die Business Keeper AG auf ihrer Homepage direkte Links zu ausgewählten Hinweisgebersystemen, bei denen die Kunden zugestimmt haben, unter <https://www.business-keeper.com/de/hinweisgebersystem/fuer-hinweisgeber.html> an.

Hinweisabgabe

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

³ Stand dieser und nachfolgender Weblinks und URLs: August 2015.


UNTERNEHMEN Musterfirma AG


Zurück
Fenster schließen

Wählen Sie bitte aus der folgenden Liste den Schwerpunkt oder Eintrag aus, der am besten auf Ihre Meldung zutrifft, und klicken Sie auf „Weiter“.

Wenn Sie zu Themen außerhalb der hier angezeigten Bereiche berichten, könnte Ihre Meldung vom System abgewiesen werden.

Bitte treffen Sie links Ihre Auswahl.
Für eine genaue Erklärung und Beispiele zu Ihrer Auswahl klicken Sie bitte auf „i“.

- Korruption** i
 Korruptives Handeln liegt vor, wenn
 - ein öffentliches Amt, eine Funktion in der Wirtschaft oder ein politisches Mandat
 - zugunsten eines anderen
 - auf dessen Veranlassung oder aus Eigeninitiative
 - zur Erlangung eines Vorteils für sich oder einen Dritten mit Eintritt oder in Erwartung des Eintritts eines Schadens oder Nachteils für die Allgemeinheit (in amtlicher oder politischer Funktion) oder für ein Unternehmen (in wirtschaftlicher Funktion) missbraucht wird.*Beispiele: Bestechung und Bestechlichkeit, unangemessene Beziehungen zu Verkäufern oder Kunden, Missbrauch vertraulicher Informationen*
- Betrug** i
- Untreue** i
- Diebstahl** i
- Unterschlagung** i
- Fehlerhafte Buchführung** i
- Urheberrechtsverletzungen** i
- Urkundenfälschung** i
- Sabotage oder Zerstörung** i
- Fehlen oder Verletzung von Sicherheitsvorschriften** i
- Diskriminierung oder Belästigung** i
- Verletzung von Richtlinien** i
- Anfragen** i
- Sonstiges** i

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.

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 Dokument der Accountspezifikationen sowie in Schulungen auf die rechtskonforme Systemeinrichtung sensibilisiert.

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

Betreff: * * Pflichtfeld

Bitte beschreiben Sie den Vorfall so detailliert wie möglich: *

Um Ihre Anonymität zu wahren, sollten die Angaben keine Rückschlüsse auf Ihre Person zulassen.

Sie haben noch 4096 Zeichen zur Verfügung.

Beantworten Sie zur optimierten Bearbeitung Ihrer Meldung zusätzlich folgende Fragen, auch wenn Sie die Antworten bereits im Textfeld genannt haben:

Sind Sie Mitarbeiter(in) der betroffenen Organisation? * Ja Nein Keine Angabe

Sind leitende Angestellte in den Vorfall verwickelt? Ja Nein Unbekannt

Sind leitende Angestellte in Kenntnis des Vorfalls? Ja Nein Unbekannt

Wie hoch ist der Gesamtschaden in Euro ungefähr? * - Schadenshöhe wählen - ▼

Seit wann besteht der Vorfall? * - Zeitraum wählen - ▼

Wann haben Sie den Vorfall bemerkt? * - Zeitraum wählen - ▼

In welchem Bereich ereignet sich der Vorfall? - Bereich wählen - ▼

Bitte geben Sie die genaue Bezeichnung der Abteilung an:

Welche weiteren Organisationen sind an dem Vorfall beteiligt?

Name:	Ort:	Organisationsform:
		- Bitte wählen - ▼

Anhang: Sie können eine Datei bis zu einer Größe von 2 MB senden.

Hinweis zum Versand von Anhängen: Dateien können versteckte personenbezogene Daten enthalten, die Ihre Anonymität gefährden. Entfernen Sie diese Daten vor dem Versenden. Sollten Sie diese Daten nicht entfernen können, kopieren Sie den Text Ihres Anhangs zu Ihrem Meldungstext oder senden Sie das gedruckte Dokument anonym unter Angabe der Referenznummer, die Sie am Ende des Meldungsprozesses erhalten, an die Anschrift des Hinweisempfängers (siehe Fußzeile).

Hinweis zur Kenntnis genommen.

Durchsuchen...

Wenn Sie mehrere Dateien übermitteln möchten, richten Sie sich am Ende dieses Meldevorgangs einen geschützten Postkasten ein. Dort können Sie weitere Anhänge als Ergänzung senden.

Abbildung 2 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. 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. Darüber hinaus gibt es die Rolle des Administrators zur Hinterlegung von Textbausteinen sowie des Systemadministrators für die Verwaltung der Berechtigungen.

Frühwarnsystem

Das 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 des BKMS® Systems 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

Das BKMS® System bietet Datenauswertungen, wie z.B. Logreports zur Auswertung der Systemzugriffe oder Standardreports mit nicht-personenbezieharen 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

Eine Meldung kann nur durch einen befugten Bearbeiter gelöscht werden. Hierzu muss zunächst die Meldung als abgeschlossen markiert werden, was eine Kommentierung durch den Bearbeiter erfordert. Erst dann kann ein anderer befugter Bearbeiter für diese Meldung ebenfalls unter Angabe eines Kommentars die Löschung ablehnen oder freigeben (4-Augen-Prinzip).

Es besteht dann die Möglichkeit, die Meldung zu archivieren. Das bedeutet, dass diese in die IT-Struktur des Anwenders per Download kopiert wird. Wenn die Löschfreigabe erteilt ist, kann ein Benutzer mit der notwendigen Berechtigung die Meldung im BKMS® System endgültig löschen.

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 des BKMS® Systems für 3 Jahren aufbewahrt, um längeren Revisionen, Gerichtsverfahren und Verjährungsfristen entsprechen zu können. Auf Wunsch des Anwenders können kürzere Löschfristen von 1 Jahr 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 kann Textbausteine, die bei der Meldungsbearbeitung verwendet werden können, 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 im BKMS® System sehr detailliert abstimmen.

Über eine SSH-Schnittstelle greift die Business Keeper AG auf die Server des BKMS® Systems zu Wartungs- und Backupzwecken zu, wobei ein Zugriff auf Meldungsinhalte des Anwenders nicht möglich ist.

Verantwortliche Stelle und Auftragsdatenverarbeiter

Der Anwender des BKMS® Systems ist als datenschutzrechtlich verantwortliche Stelle einzuordnen. Werden im Rahmen des BKMS® Systems 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

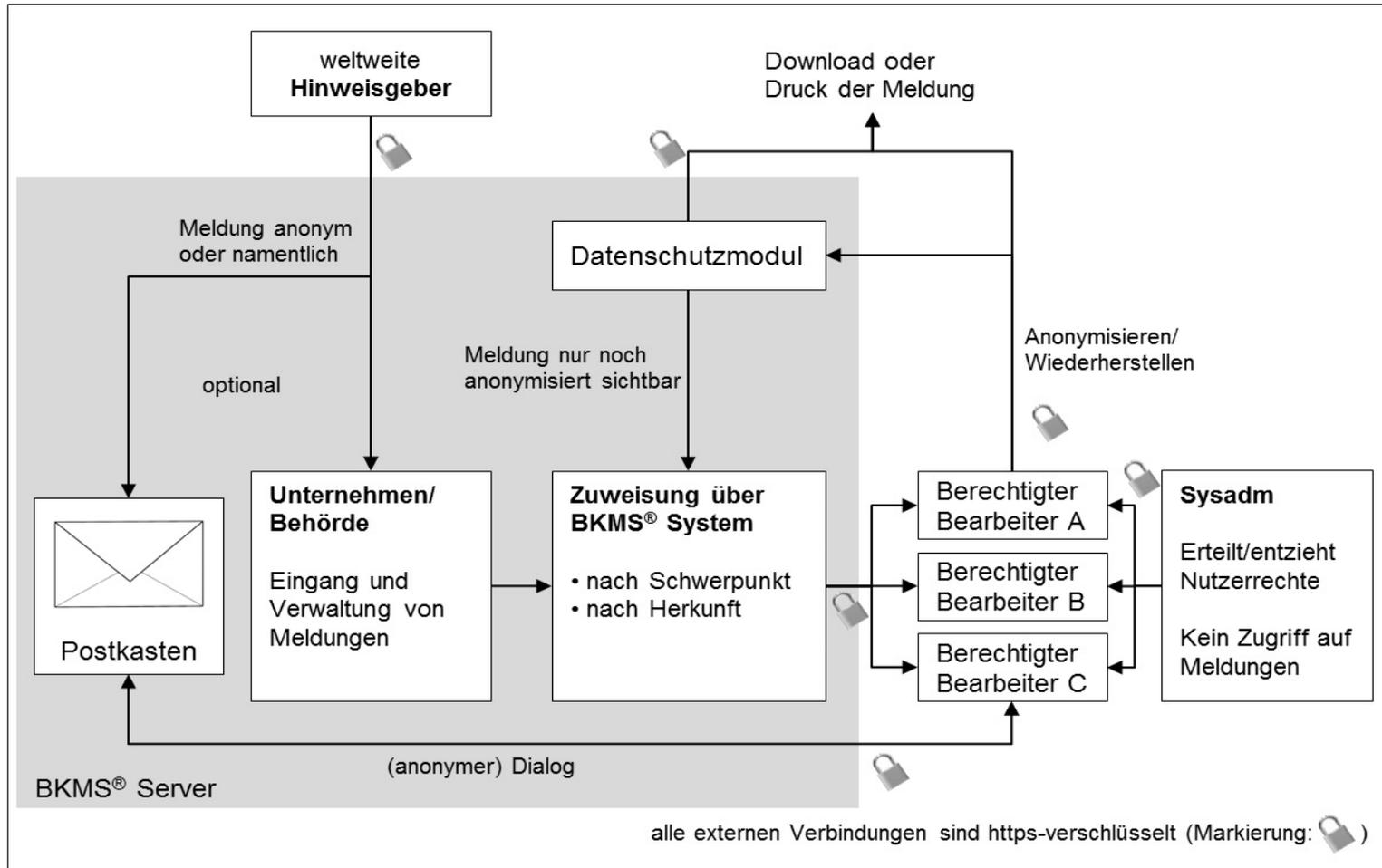


Abbildung 3 Datenflussdarstellung

10. Version des der Prüfung zugrunde gelegten Anforderungskatalogs

Version 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)⁴, 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-Korruptionskonvention⁵ oder § 11 Geldwäschegesetz, § 10 Wertpapierhandelsgesetz, § 16 Abs. 1 Arbeitsschutzgesetz sowie Remonstrationspflichten im Beamtenrecht. Denkbar sind ferner individuelle oder kollektive Vereinbarungen über Hinweise bei Regelverstößen.

Dabei ist hervorzuheben, dass ausländische bzw. internationale Regelungen, wie der SOX, keine datenschutzrechtlichem Grundlagen der Datenverarbeitung und Datenübermittlung im Sinne nationaler Datenschutzbestimmungen darstellen⁶.

Rechtsgrundlage der Datenverarbeitung und Datenübermittlung in Hinweissystemen ist vielmehr § 28 Abs. 1 S. 1. Nr. 2 Bundesdatenschutzgesetz (BDSG) 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) und die Datenschutzverordnung (DSVO) Schleswig-Holstein heranzuziehen sind.

Zudem sind die Auslegungshilfen der Artikel-29-Datenschutzgruppe der Europäischen Union, die Rechtsprechung der Europäischen Gerichtshöfe sowie ggf. nationale Vorgaben oder Auslegungshilfen der Datenschutzaufsichtsbehörden im Rahmen der Evaluation zu beachten. Diesbezüglich ist insbesondere 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*”)⁷ zu nennen, sowie die Richtlinien für die Implementierung von Whistleblowing-Systemen der französischen Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL)⁸ und der Arbeitsbericht der

⁴ Abrufbar unter <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR>.

⁵ Convention on Combating Bribery of Foreign Public Officials in International Business Transactions vom 21.11.1997 in Verbindung mit den Good Corporate Governance Principles der OECD, abrufbar unter <http://www.oecd.org/corruption/oeccantibriberyconvention.htm>.

⁶ Dies ist die überwiegende Rechtsauffassung, vgl. auch Working Paper No. 117 der Art-29-Datenschutzgruppe.

⁷ Abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

⁸ 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.

deutschen Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises zum Thema „Whistleblowing – Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“⁹.

Hervorzuheben ist, dass der Hersteller des BKMS® Systems 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. LDStG S-H zulässig, wenn sie vertraglichen Zwecken dienen, auf einer ausdrücklichen Einwilligung beruhen oder im berechtigten Interesse einer Organisation oder eines Unternehmens erfolgen, ohne dass schutzwürdige Interessen der Betroffenen dem entgegenstehen. Hierbei ist zu berücksichtigen, dass gemeldete Daten personenbezogen oder zumindest 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 kann¹⁰. Das Einwilligungserfordernis kann allerdings im 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 das 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

⁹ Abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=246.

¹⁰ Siehe hierzu Abschnitt D. 4 des Arbeitsberichts der deutschen Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises zum Thema „Whistleblowing – Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“.

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 des BKMS® Systems ermöglichen.

Auch die Verarbeitung personenbezogener 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

Das 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.

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. Auskunftersuchen oder Widerruf von Einwilligungen, können durch das BKMS® System unterstützt werden durch schnellen Datenzugriff und Auswertungen.

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

Die Vertraulichkeit der Daten wird beim 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 des BKMS® Systems 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 Re-Zertifizierung.

Bremen, 01. August 2015



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



Ralf von Rahden
datenschutz cert GmbH