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

im Auftrag der Business Keeper AG

datenschutz cert GmbH
7. Dezember 2017

Inhaltsverzeichnis

1. Über dieses Kurzgutachten

Mit diesem Kurzgutachten wird die Auditierung des IT-Produkts „Business Keeper Monitoring System (BKMS® System)“ in der leicht veränderten 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 Datenschutzgütesiegelverordnung (DSGSVO)[1] in Schleswig-Holstein, welches durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) vergeben wird.

Hervorzuheben ist, dass das BKMS® System im Rahmen eines Kombiverfahrens auch gemäß dem Gütesiegelstandard „EuroPriSe“ (European Privacy Seal)[2] seitens der Experten der datenschutz cert GmbH geprüft und durch die EuroPriSe GmbH zertifiziert wurde.

2. Zeitraum der Prüfung

Die Begutachtung erstreckte sich auf den Zeitraum von 31.07. bis 07.12.2017 und beinhaltete neben der konzeptionellen Analyse der zur Verfügung gestellten Dokumente und der Befragung von Projektverantwortlichen auch die Durchführung von Plausibilitäts- und Funktionstests im System selbst.

3. Antragstellerin

Antragstellerin dieses Gutachtens ist die

Business Keeper AG,
Bayreuther Straße 35,
10789 Berlin

als Hersteller und Anbieter. Ansprechpartner ist Herr Kenan Tur, Vorstand der Business Keeper AG. Projektverantwortliche ist Frau Stephanie Gouze, betriebliche Datenschutzbeauftragte der Business Keeper AG.

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 Alexey Testsov (Technik).

---

[1] Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) v. 30.11.2013, GVOBl. Schl.-H. 2013, S.536ff.

[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 die EuroPriSe GmbH. Weitere Informati0nen sind abrufbar unter https://www.european-privacy-seal.eu/ (Stand Dezember 2017).

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

56c6da4f4fa1659c2c15d4dace80b7eec0936f90f973e05be9a24f972cd4c26c

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 Rechenzentren in Deutschland und der Schweiz betrieben. Unter Anwender wird im Folgenden allgemein der Kunde der Business Keeper AG verstanden, der das BKMS® System einsetzt. Dazu gehören autorisierte Benutzer des Kunden wie Meldungsbearbeiter und Systemadministratoren. Hinweisgeber gehören entsprechend dieser Definition nicht zu Anwendern. Der IT-Service wurde mit Stand zum Dezember 2017 auditiert.

6. Beschreibung des IT-Produkts

Das BKMS® System (Hinweisgebersystem) ist das Kern-Modul des BKMS® Compliance Systems. Das BKMS® System ist eine webbasierende Anwendung. Der Anwender entscheidet, ob das

- --- 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 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. Die verantwortliche Stelle kann ferner auch externe Personen (z.B. Ombudsleute, Wirtschaftsprüfer) außerhalb des Anwenders in den Dialog bzw. in die Meldungsbearbeitung im BKMS® System 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 Loadbalancer, vier Anwendungsservern, einem Datenbankserver sowie ein Entwicklungs- und Testsystem. Nicht zum Auditgegenstand gehören die anderen Module (BKMS® VoiceIntake, BKMS® Case Management und BKMS® Third Party), die Einsatzumgebung beim Anwender, die spezifische Konfiguration von BKMS® System beim Anwender, insbesondere die Rolle des externen Übersetzers, die Einrichtung oder Nutzung Individueller Reports, die Einrichtung oder Nutzung von Themen, die Einrichtung oder Nutzung von Hinweistexten oder Einwilligungserklärungen im Rahmen der Hinweisabgabe, die Datenlöschung sowie die Lizenzierung und Vertriebsprozesse

bei der Business Keeper AG und weitergehende Service- oder Beratungsleistungen der Business Keeper AG.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Es wurden keine für die Bewertung relevanten Tools eingesetzt.

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 Anmeldemaske für Meldungsbearbeiter und Systemadministratoren ist unter https://client.bkms-system.net/bkwebanon/action/client/clientDisclaimer.do?language=ger erreichbar[3]. 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. Zusätzlich bietet die Business Keeper AG auf ihrer Homepage Links zu Hinweisgebersystemen an.

[3] Stand dieser und nachfolgender Weblinks und URLs: Dezember 2017.

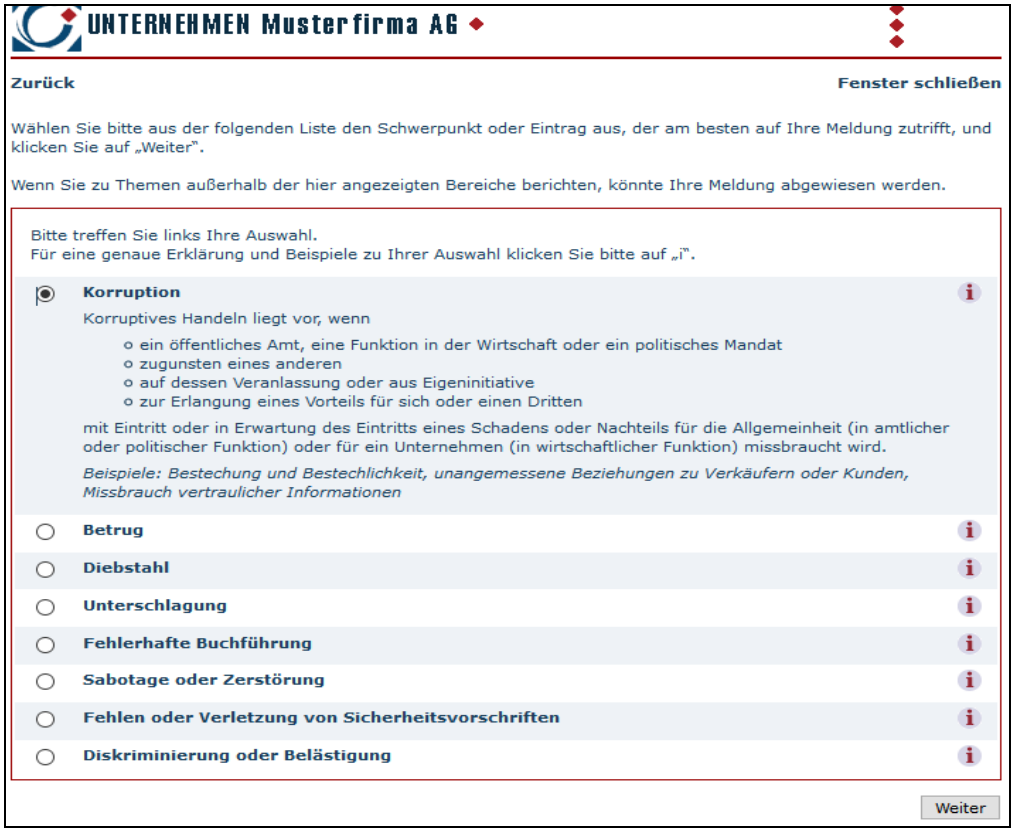


Abbildung 1: Ausschnitt aus der Anmeldemaske zum BKMS® System

Hinweisabgabe

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

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.

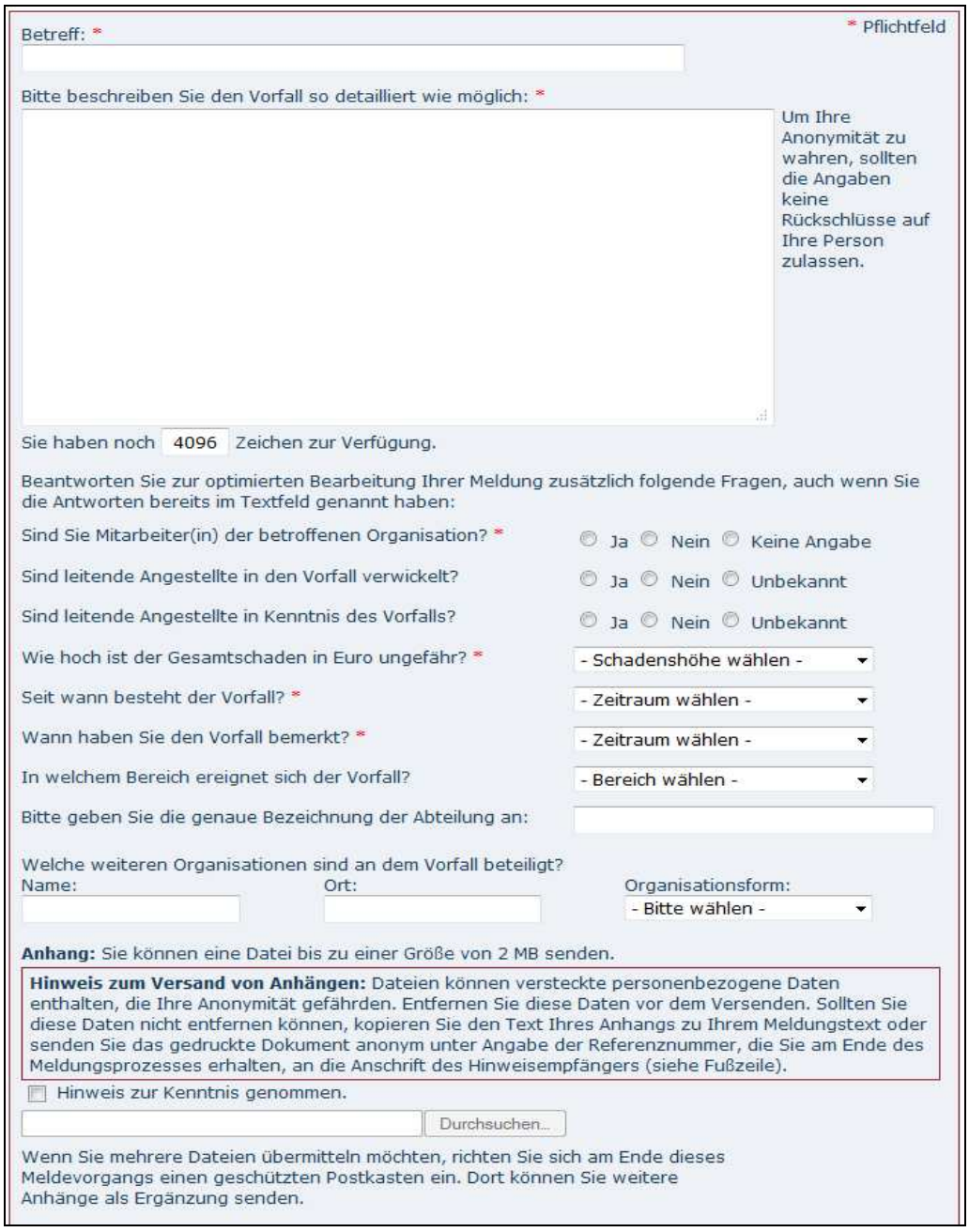


Abbildung 2 Datenerfassungsmaske für Hinweisabgabe

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 sodann 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. 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 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.

Für den Abschluss von Meldungen wurde zudem das 4-Augen-Prinzip eingeführt, was die Sicherheit der berechtigten Zugriffe erhöht.

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 entsprechend seiner Berechtigungen bearbeiten. Darüber hinaus gibt es die Rolle des Administrators zur Hinterlegung von Textbausteinen sowie des Systemadministrators für die Verwaltung der Berechtigungen.

Um die Zugriffsrechte detaillierter vergeben zu können, wurde die Bearbeiter-DatenPIN als Standardfunktion eingeführt. Sie ermöglicht eine individuelle Vergabe der DatenPIN (im Vergleich zu einer gemeinsamen DatenPIN mehrerer Bearbeiter) und minimiert somit das Missbrauchsrisiko durch Unbefugte. Bei Ausscheiden eines Bearbeiters aus dem Unternehmen muss dann nur das Benutzerprofil dieses Bearbeiters deaktiviert und gelöscht werden.

Diese Maßnahmen haben die positive Auswirkung auf die Sicherheit des Produktes.

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 Auftragsdaten-verarbeitung zu qualifizieren.

Auditor

Neu ist die Funktion eines kundenspezifischen Benutzertypus „Auditor“, der nur Leserechte auf die vom Anwender bestimmten Bereiche erhält, z.B. auf das Aktivi-tätslog, Revisionsprotokoll oder die Benutzerverwaltung. Der Auditor hat keinen Zugriff auf Meldungen. Bereiche werden vom Systemadministrator freigeschaltet. Auch dies hat positive Auswirkung auf die Sicherheit des Systems.

Auswertungsmöglichkeiten

Das 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. Die Datenverarbeitung für Anwender erfolgt datentechnisch separiert. Zusätzlich wird die Datentrennung durch die Verschlüsselung ergänzt.

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 auf Wunsch des Anwenders zu archivieren. Diese Archivfunktion gehört nicht mehr zum Standardumfang. 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.

Die Benutzerverwaltung wurde seit der letzten Zertifizierung um eine Übersicht für den Sysadmin ergänzt. Ferner wurde für die Verwaltung der Benutzer eine neue Registerkarte „Rollen Meldungsbearbeitung“ als Übersicht hinzugefügt, was die Benutzerfreundlichkeit fördert.

Administration des BKMS® Systems

Der sogenannte Administrator (Admin) des Anwenders übernimmt untergeordnete Aufgaben und kann lediglich Textbausteine, die bei der Meldungsbearbeitung verwendet werden können, erstellen und bearbeiten. Der vom Anwender definierte Systemadministrator (Sysadm) erteilt oder entzieht Zugangsberechtigungen und kann Hinweisbearbeiter einrichten, ändern oder löschen. Dabei hat er keinen Zugriff auf Meldungsinhalte. Der Sysadm kann Rechte im BKMS® System sehr detailliert abstufen und in der neuen Funktion „Einstellung Benutzerkennwort“ die Vorgaben für die zeitliche Frist zum Wechsel des Passwortes und die Anzahl der Wiederverwendungen eines vorherigen Passwortes setzen. 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 Auftrags(daten)verarbeiter

Der Anwender des BKMS® Systems ist als 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 Auftrags(daten)verarbeiter. Hervorzuheben ist, dass das Unternehmen im Rahmen des SaaS nur auf verschlüsselte Daten zugreifen

könnte. Die eingesetzten Rechenzentrumsdienstleister haben keinen Zugriff auf die Daten im BKMS® System. Mitarbeiter des jeweiligen Rechenzentrums übernehmen keine administrativen Funktionen im Zusammenhang mit dem BKMS® System; die Rootrechte liegen ausschließlich bei der Business Keeper AG.

9. Modellierung des Datenflusses

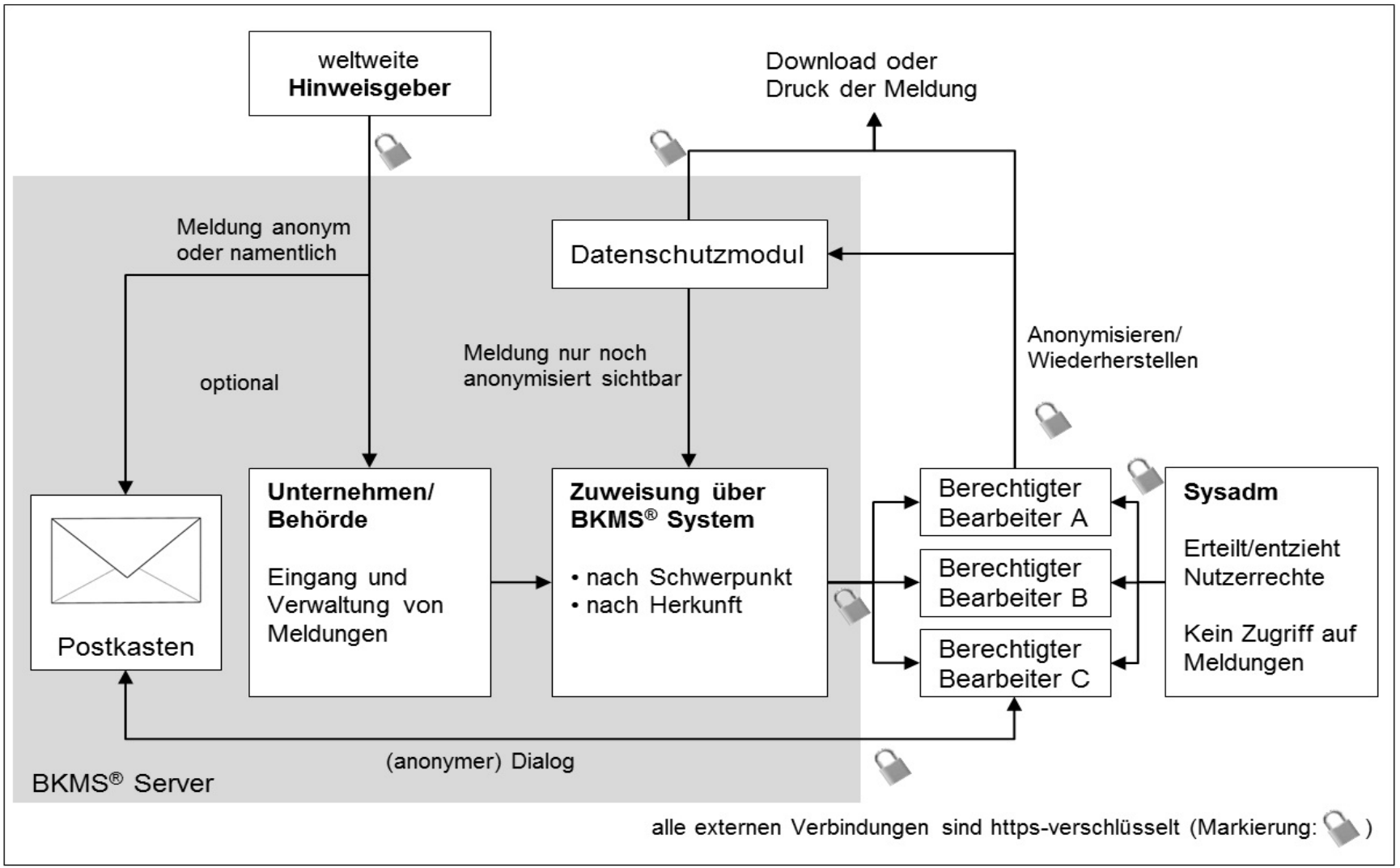


Abbildung 3 Datenflussdarstellung

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), 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 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 datenschutzrechtlichen Grundlagen der Datenverarbeitung und Datenübermittlung im Sinne nationaler Datenschutzbestimmungen darstellen[4].

Rechtsgrundlage der Datenverarbeitung und Datenübermittlung in Hinweissystemen ist vielmehr der zum Auditzeitpunkt noch gültige § 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.

Hervorzuheben ist, dass das BKMS® System im Rahmen des Audits zugleich auf die Einhaltung der Anforderungen der EU-Datenschutzgrundverordnung (DSGVO) geprüft wurde. Dabei ist Art. 6 Abs. 1 Satz 1 lit. f DSGVO als Rechtsgrundlage der Datenverarbeitung heranzuziehen Die Business Keeper AG hat zum Auditzeitpunkt bereits ein DSGVO-konformes Datenschutz- und IT-Sicherheitsmanagement. Zu den Einzelheiten sei auf den Evaluationsbericht gemäß EuroPriSe verwiesen.

Erwähnenswert ist die Richtline (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Sie schützt zwar Geschäftsgeheimnisse, stellt aber weder Strafen für Whistle-Blower auf, noch verbietet sie Datenerfassung in Whistle-Blowing Systemen[5]. Dazu heißt es in Erwägungsgrund Nr. 20: „*Die in dieser Richtlinie vorgesehenen Maßnahmen, Verfahren und*

---

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

[5] Siehe dazu den Blogbeitrag von Conrad unter https://www.datenschutz-notizen.de/schutz-der-geschaeftsgeheimnisse-versus-whistleblowing-1515386/ .

Rechtsbehelfe sollten nicht dazu dienen, Whistleblowing-Aktivitäten einzuschränken."

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*")[6] zu nennen, sowie die Richtlinien für die Implementierung von Whistleblowing-Systemen der französischen Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL)[7] und der Arbeitsbericht der deutschen Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz" des Düsseldorfer Kreises zum Thema „*Whistleblowing – Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz*"[8]. Ferner hat der Europäische Datenschutzbeauftragte seinen Leitfaden mit Verfahrensregeln zum Umgang mit externen sowie internen Whistleblowern („*Guidelines on processing personal information within a whistleblowing procedure*") veröffentlicht[9], welcher die zuvor erwähnten Grundsätze der Aufsichtsbehörden wiederholt.

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. LDSG S-H (bzw. Art. 6 DSGVO) grundsätzlich 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 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[10]. Das Einwilligungserfordernis kann allerdings im BKMS® System auch ent-

---

[6] Abrufbar unterhttp://ec.europa.eu/justice/data-protection/article-29/index_en.htm.
[7] 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.
[8] Abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=246.
[9] „*Guidelines on processing personal information within a whistleblowing procedure*" vom 18.07.2016, abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-07-18-_Whistleblowing_Guidelines_EN.pdf .
[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.

fallen, 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 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 und Eingabemasken sind per https verschlüsselt und damit vor unbefugtem Auslesen der Kommunikation während der Datenübertragung angemessen geschützt. Ferner werden Abrufe von http auf https immer umgelenkt, so dass die Verbindung immer verschlüsselt erfolgt. Auch ist ein Framing (Aufruf des Systems in einem Frame nach Klick auf eine Verlinkung beim Kunden) technisch unterbunden, was die Sicherheit erhöht.

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 personenbeziehbarer Protokolldaten des Anwenders (Hinweisbearbeiter oder Sysadm) 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 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 Rechenzentren in Deutschland und der Schweiz, in denen sich die Komponenten von BKMS® System auf Wunsch des Kunden befinden, weisen ein hohes Maß an physikalischer Sicherheit aus und sind alle gemäß ISO/IEC 27001 zertifiziert. Die Server werden mit sehr 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 den datenschutzrechtlichen Anforderungen entspricht. Auch die Unteraufträge der eingesetzten Rechenzentrumsdienstleister erfüllen diese Anforderungen.

Das Informationssicherheits-Managementsystem (ISMS) für den Geltungsbereich Sicherer Betrieb des BKMS® Compliance Systems wurde gemäß den Anforderungen der internationalen Norm ISO/IEC 27001:2015 zertifiziert (Zertifikat der datenschutz cert GmbH, DSC.501.11.2017, gültig bis 22.11.2020).

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. Auskunft 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

BKMS® System enthält folgende, den Datenschutz fördernde Funktionen:

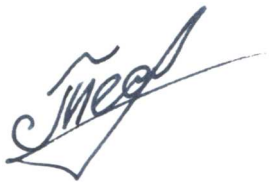
- Die Vertraulichkeit der Daten wird durch ein Berechtigungskonzept, das die Vergabe sehr differenzierter Zugriffsrechte ermöglicht, sichergestellt.
- Service-Beschreibungen und Informationen zur Datenverarbeitung sind vorbildlich transparent und ermöglichen die Umsetzung der Betroffenenrechte in optimaler Weise;
- Organisatorische und technische Maßnahmen, die der Auftragnehmer zur Datensicherheit und zum Datenschutz trifft, gehen über die gesetzlichen Anforderungen hinaus.
- Der Auftragnehmer sensibilisiert den Anwender in vorbildlicher Weise auf die Einhaltung des Datenschutzes, u.a. durch ein Datenschutzhinweisblatt.
- Die Rechenzentren, in denen sich die Komponenten von BKMS® System befinden, weisen ein hohes Maß an physikalischer Sicherheit aus.

- Die seitens der Business Keeper AG entwickelten und umgesetzten Datenschutz- und Sicherheitsmaßnahmen entsprechen vorbildlich dem Privacy-by-Design Grundsatz.

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, 7. Dezember 2017



Alexey Testsov
datenschutz cert GmbH

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