# Short Public Report

# on the IT-based service

# BKMS® System

## 1. Name and version of the IT-based service:

| | |
|---|---|
| IT-based service: | BKMS® System (Business Keeper Monitoring System). |
| Version: | 2.7.3. |
| Functional status: | May 2013. |

## 2. Manufacturer / vendor and Provider of the IT-based service:

| | |
|---|---|
| Company Name: | Business Keeper AG |
| Company Address: | Bayreuther Straße 35, 10789 Berlin, Germany |
| | Web: www.business-keeper.com |
| Contact Person: | Mr. Kenan Tur |

3. **Time frame of evaluation:** 2012/11/27 – 2013/06/03

## 4. EuroPriSe Experts who evaluated the IT-based service:

| | |
|---|---|
| Name of the Legal Expert: | Dr. Irene Karper |
| Address of the Legal Expert: | datenschutz cert GmbH<br>Konsul-Smidt-Str. 88a<br>28217 Bremen, Germany |
| | ikarper@datenschutz-cert.de |
| Name of the Technical Expert: | Ralf von Rahden |
| Address of the Technical Expert: | datenschutz cert GmbH<br>Konsul-Smidt-Str. 88a<br>28217 Bremen, Germany |
| | rrahden@datenschutz-cert.de |

## 5. Certification Body:

| | |
|---|---|
| Name: | Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig Holstein<br>(Independent Centre for Privacy Protection (ULD) Schleswig-Holstein |
| Address: | Holstenstr. 98<br>24103 Kiel, Germany |
| eMail: | europrise@datenschutzzentrum.de |

## 6. Specification of Target of Evaluation (ToE):

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.

Diese Varianten beschreiben lizenzbedingte Konstellationsmöglichkeiten von BKMS® System und wurden gemeinsam als BKMS® System evaluiert.

Zum ToE gehört ein Produktivsystem mit einem Loadbalancer, zwei Anwendungsservern und einem Datenbankserver sowie ein Entwicklungs- und Testsystem.

## 7. General description of the IT-based service:

BKMS® System ermöglicht einen Dialog zwischen Hinweisgebern und Hinweisbearbeitern, um Missstände, Gefahren oder Risiken melden zu können und wird als „Whistleblowing“-System zur Unterstützung des Wertemanagements, der Compliance oder der Revision eingesetzt.

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.

BKMS® System kann im Rahmen des Customizings auf die Bedürfnisse des Anwenders zugeschnitten werden. Die Business Keeper AG sensibilisiert den Anwender auf die Einhaltung datenschutzrechtlicher Vorgaben bei einer individuellen Konfiguration, z.B. durch Merkblätter und Schulungen.

Da dem Anwender weder Hard- noch Software zur Verfügung gestellt wird, sondern ein webbasierender Service, handelt es sich bei BKMS® System nicht um ein IT-Produkt, sondern um einen IT-basierenden Service.

## 7.1 Purpose and area of application

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 ist unter https://www.business-keeper.com/kundenlogin.html erreichbar (June 2013). Üblicher Weise verlinken Anwender den Zugang zum BKMS® System allerdings auf ihren eigenen Homepages.

**Hinweisabgabe**

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

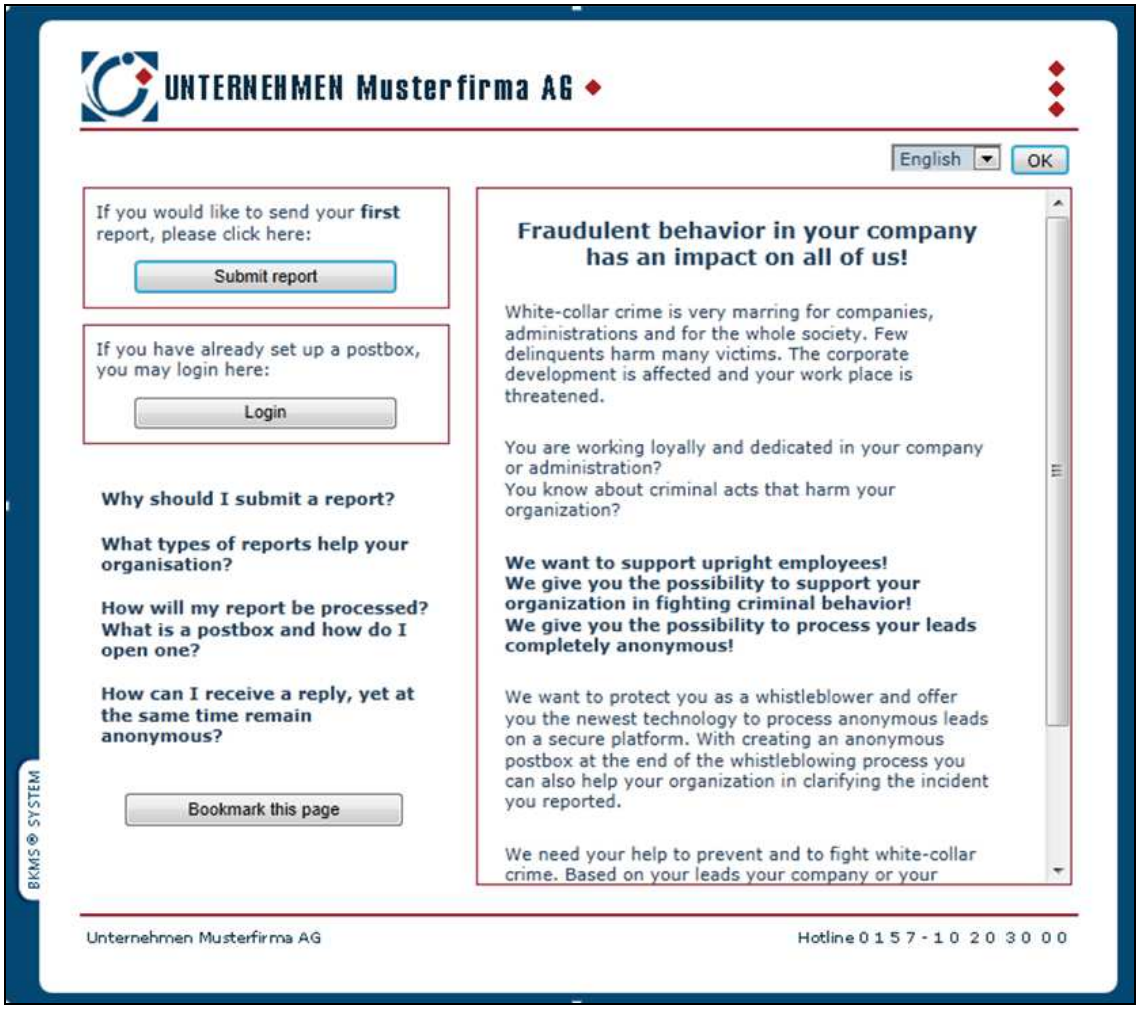


Illustration 1 Part of the Test-User-Homepage of BKMS® System

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

Der Hinweisgeber wird dann auf bestimmte Melde-Themen geleitet.

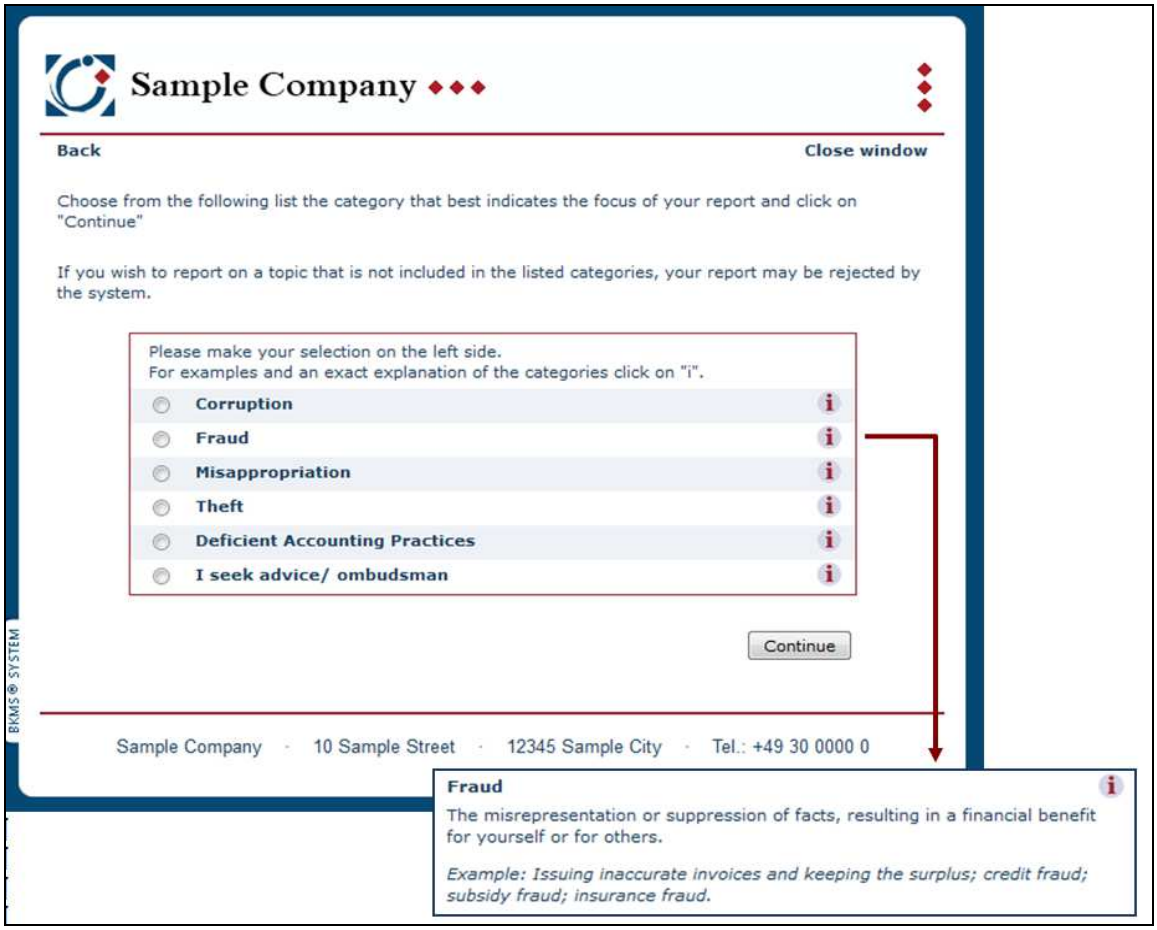


Abbildung 2 Beispiel für Melde-Themen

Die Definition der Melde-Themen erfolgt durch den Anwender anhand der für ihn geltenden Gesetze oder Regelungen. Die seitens der Business Keeper AG in der Standardausführung vorgegebenen Meldethemen beziehen sich dabei insbesondere auf Straftaten, nicht aber auf Verstöße gegen Verhaltensweisen, welche unternehmensinterne Ethik- und Verhaltensregeln beeinträchtigen, da hier in der Regel das schutzwürdige Interesse der Betroffenen gegen eine Datenerfassung spricht. Der Anwender kann gleichwohl derartige Melde-Themen konfigurieren. Er wird auch hier 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.

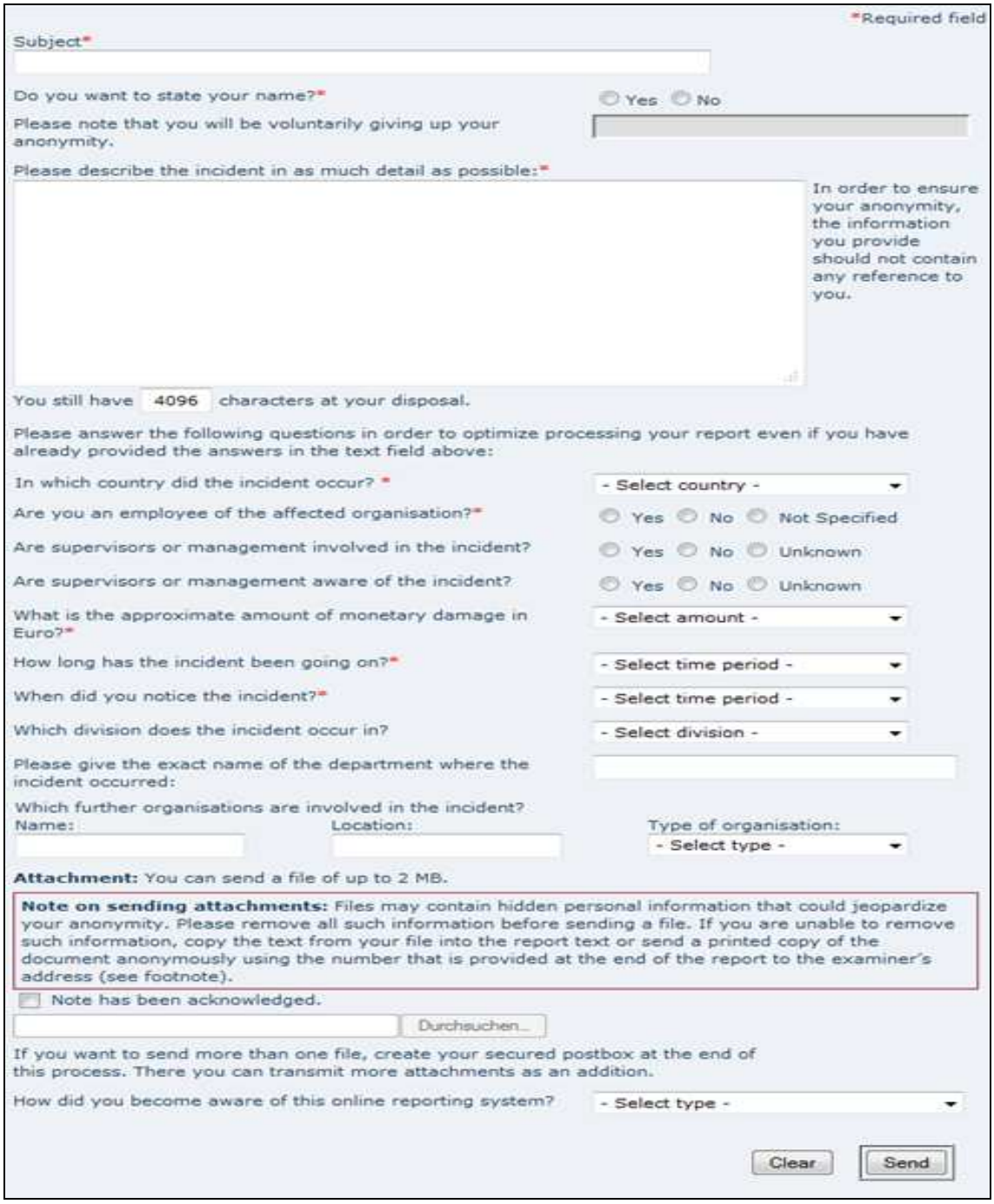


Abbildung 3 Datenerfassungsmaske für Hinweisabgabe

Anwender können für die Formulareingabe Schlüsselwörter definieren, die als unzulässig ausgefiltert werden (z.B. Beleidigungen). Ist ein als unzulässig definierter 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 verwaltet und bearbeitet wird. Die Meldung kann zudem ausgedruckt werden.

**Postkasten**

Nur an dieser Stelle kann der Hinweisgeber 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. Mit Abschluss wird der Postkasten verschlüsselt und eine Postkasten-ID („PID“) 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.

Zur Accountaktivierung und -nutzung wird als zusätzlicher Sicherheitsaspekt bei der Zuordnung von Berechtigungen eine „DatenPIN“ benötigt. Sie wird verschlüsselt in der Datenbank abgelegt. 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.

Der Hinweisbearbeiter erhält nach Login eine Statusübersicht und kann Meldungen z.B. sortieren oder auf Wiedervorlage legen.

**Frühwarnsyste**m

BKMS® System enthält zudem 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.

**Privacy Function**

Bei der sogenannten „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 und damit von der Evaluation umfasst ist die optional konfigurierbare Rolle eines externen Übersetzers, für den Meldungen zur Übersetzung freigegeben werden können. Die Rolle externer Übersetzer ist als Auftragsdatenverarbeitung zu qualifizieren.

**Auswertungsmöglichkeiten**

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

**Verschlüsselung der Daten**

Zur Verschlüsselung der Meldungen wird ein asymmetrisches Kryptosystem (Public-Key-Verfahren) eingesetzt. Das Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, wird zusätzlich durch eine Passphrase ergänzt, welche auf die Business Keeper AG sowie auf den Anwender verteilt aufbewahrt wird. Auf diese Weise wird sichergestellt, dass die Business Keeper AG keinen Zugriff auf die Inhalte der Meldungen hat.

Eine Meldung kann nur unter Eingabe der DatenPIN entschlüsselt werden.

Für BKMS® System ist eine Mandantentrennung eingerichtet. Unterschiedliche Datenbanken pro Anwender sowie die Verschlüsselung setzen die Datentrennung endgültig um.

**Archivierung und Löschung**

Meldungen können durch befugte Bearbeiter gelöscht oder archiviert werden.

Bei Löschung eines Benutzers werden diesem alle Rechte entzogen. Name, Vorname und Alias/Kürzel bleiben erhalten, um Alias-Doubletten zu verhindern und Aktivitäten im Log dadurch 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 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 Stellen in größerem Umfang über die Bearbeitung oder Bewertung eines Hinweises (mit-)entscheiden. Erhalten sie hierfür Hinweise oder Daten mittels BKMS® System, handelt es sich um eine Datenübermittlung.

Die Business Keeper AG ist als Auftragsdatenverarbeiter zu qualifizieren. Hervorzuheben ist, dass das Unternehmen im Rahmen des software as a service nur auf verschlüsselte Daten zugreifen könnte. Dies gilt auch für die Telekom Deutschland GmbH, die im Unterauftrag das Rechenzentrum in Deutschland betreibt. Die Business Keeper AG hält für Kunden ein Vertragskonvolut zur Verfügung, welches die Anforderungen an eine schriftliche Regelung erfüllt. Auch der Unterauftrag zwischen der Business Keeper AG und der Telekom Deutschland GmbH erfüllt diese Anforderungen.

### 7.2 Audited range of functions in the standard version

BKMS® System in the audited version 2.7.3 includes the functional status May 2013 on SHA256,

bd4570f7bb1e2171c246dac7a137e395988c2bde55c85e16b8e986e091e83495.

The range of the standard version also includes the IT-based service of Business Keeper AG on behalf of the user, in particular hosting BKMS® System.

### 7.3 Functions outside the approved standard

Not part of the scope of BKMS® System evaluation were the following issues:

- Special configuration by users, especially regarding the role as an external translator, the implementation or utilization of individual reports as well as non-standardised topics, text or explicit consent in data processing,
- provision of services other than BKMS® System by Business Keeper AG
- the accounting processes between Business Keeper AG and the users
- the environment for the user and sender of evidence.

## 8. Transnational issues:

Since BKMS® System is a web based application it can be used worldwide. Some deploy BKMS® System at their branches within the European Union, the EEA or worldwide.

System and server of BKMS® System are located in a data center within the Federal Republic of Germany.

## 9. Tools used by the manufacturer / provider of the IT-based service:

None.

## 10. Edition of EuroPriSe Criteria used for the evaluation:

The experts used EuroPriSe Criteria Catalogue, version November 2011.

Note: Alongside the evaluation according to EuroPriSe, BKMS® System was also evaluated according to the standard of the privacy seal due to the federal state order of Schleswig-Holstein on a privacy audit (Schleswig-Holsteinische Landesverordnung über ein Datenschutzaudit, DSAVO).

## 11. Evaluation results:

The following outstanding results could be found within the framework of the audit:

### 11.1 Implementation of legal requirements

Within the European Union (EU), Directive 95/46/EC – especially Art. 7 lit. f ii) and Directive 2002/58/EC must be observed as a framework for data protection by using BKMS® System to report grievances. National legal standards can also contain provisions for data protection, such as Section 28 of the Federal Data Protection Act (BDSG) or, as a more specific legal standard for employee data protection, Section 32 BDSG.

Furthermore, the guidance notes of the so-called Art. 29 Data Protection Working Party of the EU must be observed. This coalition of the European Data Protection Officials has specified legal requirements of data protection in its Working Paper no. 117, "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". This also applies to the work report of the German Ad-hoc Working Group on Employee Data Protection for the Düsseldorf Group on the topic: "Whistleblowing Hotlines: Internal company warning systems and employee data protection".

In principle, a reporting procedure therefore is permissible as it is contractually agreed upon, based on an explicit consent or on the legitimate interests of the organisation and no protected interests of the involved standing in the way.

Bei der Umsetzung dieser Anforderungen ist zu berücksichtigen, dass alle vom Hinweisgeber gemeldeten Daten personenbezogen oder zumindest personenbeziehbar sind, soweit sie Rückschlüsse auf eine natürliche Person zulassen. Sofern Meldungen inhaltlich auf z.B. religiöse Hintergründe oder sexuelles Verhalten eingehen, werden sogar besondere personenbezogene Daten mittels BKMS® System verarbeitet.

Processing of sensitive data require an explicit consent. Attention should be paid to the fact that approval can be given effectively only voluntary and by the person affected. Since consent of an employee is not voluntary it cannot be given effectively.

Hervorzuheben ist, dass BKMS® System die Einhaltung der jeweiligen Rechtsgrundlagen nicht garantieren kann. Allerdings wird der Anwender das das Merkblatt zum Datenschutz aufgefordert, die Rechtskonformität zu überprüfen, so dass der IT-basierende Service zumindest die Sensibilisierung auf die Einhaltung datenschutzrechtlicher Grundlagen unterstützt.

Zudem kann das Einwilligungserfordernis entfallen, sofern die Daten des Betroffenen mittels BKMS® System pseudonymisiert oder anonymisiert werden. Da BKMS® System Funktionen hierfür anbietet, unterstützt es die rechtskonforme Umsetzung.

Auch schutzwürdige Interessen der Betroffenen werden durch BKMS® System angemessen berüchsichtigt, especially regarding the reporting-themes. Reports

may concern violations or statutory crimes in the areas of financial reporting, internal financial reporting controlling, questions of business auditing, corruption, banking and financial criminality or human rights violations and environmental issues (so-called hard facts). Not permissible are reports about violations of "soft facts" such as ethics or conduct regulations; these can only be justified exceptionally when no protective interests of the involved parties stand in the way. The targeted and limited request for information is achieved with the topic list and the filter function in the BKMS® System. Der Anwender wird auch auf diese Grundsätze angemessen sensibilisiert im Datenschutzmerkblatt und konfiguriert das BKMS® System abweichend von den Standardausführungen auf eigene Verantwortung.

Indem mittels BKMS® System Missstände, Gefahren oder Risiken für die Allgemeinheit abgewendet werden können, erfolgt dies zudem grundsätzlich im öffentlichen Interesse i.S. d. Art. 7 lit. e der Richtlinie 95/46/EG, 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. Der Anwender wird im Datenschutzhinweisblatt auf die für ihn ggf. geltenden Bestimmungen zur Datenübermittlung, die Vorabkontroll- und sowie Informationspflichten gemäß Art. 10 der Richtlinie 95/46/EG sensibilisiert.

Companies which transfer data to offices within the EU or the EEA can essentially assume an appropriate level of data protection and privacy rights. The situation is, however, different for data transfer to offices in third countries where a special authorisation is required. If the European Commission does not recognise an appropriate level of data protection in a third country, participation in the "Safe Harbour" standard in the USA, signing a standard contract clause of the European Commission or an officially recognised corporate-wide data protection directive can also effect an appropriate level of data protection and privacy, if applicable. Hinweisblatt, Zudem können Rollen und Berechtigungen bereits so abgestuft werden, dass eine Übermittlung nur im restriktiven Umfang möglich gemacht wird.

Auch die Vorgaben der Directive 2002/58/EC zu Cookies und zur Vertraulichkeit der Kommunikation sind eingehalten. Sowohl bei der Hinweisabgabe über Online-Formulare als auch bei der Frühwarnfunktion per SMS und E-Mail ist die Vertraulichkeit der öffentlichen Kommunikation sichergestellt. Die die Webseiten sind per https verschlüsselt und damit vor unbefugtem Auslesen der Kommunikation während der Datenübertragung angemessen geschützt. Loginfunktionen erfordern ein angemessen sicheres Passwort. Die Verschlüsselung der Daten sichert die Vertraulichkeit. Auch das Setzen eines Cookies erfolgt rechtskonform zur Directive 2002/58/EC, da somit die vom jeweiligen Teilnehmer gewünschte Nutzung von BKMS® System ermöglicht wird und kein Einwilligungserfordernis vorliegt. Also impacts on the „Position paper on the impact oft he new „cookie law“ on certifiability of behavioral advertising systems according to EuroPriSe“ from July 2010 are not affected.

BKMS® System erfasst schließlich personenbeziehbare Protokolldaten über Aktivität und Zeitpunkt. Auch diese Verarbeitung ist zulässig, da sie für die Kontrolle der berechtigten Nutzung– und damit als technisch-organisatorische Maßnahmen des Datenschutzes – erforderlich sind.

### 11.2 Data avoidance

BKMS® System allows the anonymisation of data by using the special “privacy function”. It also allows the user to delete or minimize personal data. Secondary data - such as log files – are automatically deleted within a short, sufficient time. In addition, BKMS® System provides functions to avoid or minimize processing of personal information, such as:

- anonymous statistical analysis,
- a differentiated authorization concept; access to personal data within the BKMS® System can thus be limited to need-to-know-basis.

The user is explicitly pointed towards the principles of data avoidance and data minimization by the fact sheet about information on the use of the BKMS® System in compliance with data protection rights and is asked to comply with them for the individual establishment and use of the system.

### 11.3 Data security

The servers are operated in a data center with strong admittance and access controls. All data transfers within the use of BKMS® System are secured via SSL. Also, the data is backed up appropriately following a backup policy.

Es fehlt allerdings eine Dienstanweisung zum Umgang mit Accountdaten von Mitarbeitern der BK AG nach deren Ausscheiden, wenngleich diese derzeit durch die Business Keeper AG erstellt wird.

### 11.4 Implementation of consumers‘ rights

The processor provides information on his website and in a fact sheet on the use of the BKMS® System in compliance with data protection rights that allow users to implement data subject´s rights and to react on consumer questions or e.g. dissents in data proceeding. The BKMS® System also provides a mailbox function that allows the sender of evidence to correct or delete his own personal data.

## 12. Data flow:

The following graphic describes the data flow of BKMS® System:

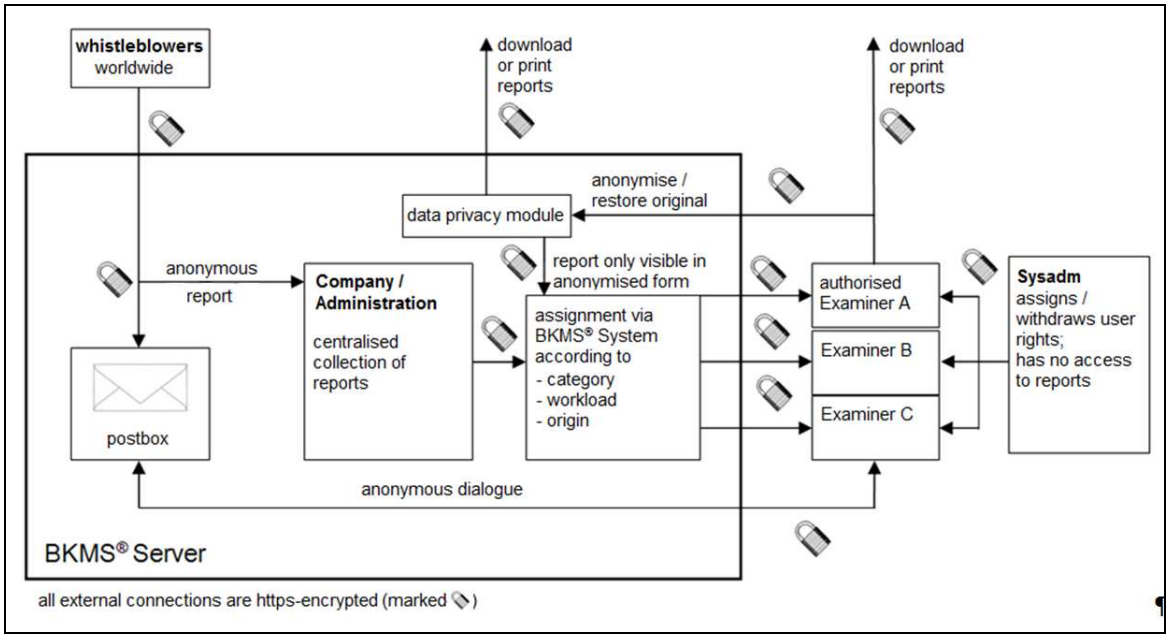


Illustration 4 data flow

Illustration 1: data flow

## 13. Privacy enhancing functionalities:

Die Vertraulichkeit der Daten wird bei BKMS® System 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.
- Das Rechenzentrum, in welchem sich die Komponenten von BKMS® System befinden, weist ein hohes Maß an physikalischer Sicherheit aus.

## 14. Issues demanding special user attention:

The evaluation did only one issue rate as “additional safeguards needed”.

## 15. Compensation of weaknesses:

BKMS® System does only one requirement with the grade “barely passing”, so there is need to compensate a shortcoming.

Es fehlt allerdings eine Dienstanweisung zum Umgang mit Accountdaten von Mitarbeitern derBusiness Keeper AG nach deren Ausscheiden, was als barely passing zu bewerten war. Um dies zu kompensieren, wurde daher die Auflage erteilt, ein solches Dokument zu erstellen. Die Business Keeper AG erarbeitet bereits ein entsprechendes Dokument.

Nevertheless the privacy compliant use of BKMS® System lies within the responsibility of the user. He must adopt the given information by the developer about privacy standards and privacy enhancing configuration of BKMS® System.

## 16. Decision table on relevant requirements:

| *EuroPriSe Requirement* | *Decision* | *Remarks* |
|---|---|---|
| Data Avoidance and Minimisation | adequate | BKMS® System allows collecting different data; data avoidance and data minimisation lies in the responsibility of the user; nevertheless BKMS® System allows the anonymisation of data by using the special “privacy function”. It also allows the user to delete personal data and deletes secondary data - such as log files - within a short, sufficient time. In addition, BKMS® System provides functions to avoid or minimise processing of personal information, such as anonymous statistical analysis or a differentiated authorization concept. Finally the data processor is sensitizing the user to fulfill data protection measures (e.g. by a fact sheet about information on the use of the BKMS® System in compliance with data protection rights. |
| Transparency | adequate - excellent | Documentation and fact sheets on behalf of compliance and privacy are informative, up-to date and understandable; the processor also provides information for security policies and a privacy concept. Information about privacy protection on the website of the processor are compliance with legal standards (German Telemedia Act). |
| Technical-Organisational Measures | excellent | Organizational and technical measures on data security and privacy are above legal standard. The data center is located in Germany and complies with all standards in regard to physical access control, recovery mechanism, network and transport security on a high level. The IT infrastructure is well-documented; a security policy is in place. Employees are well trained on privacy and data security matters. |

| | | |
|---|---|---|
| Data Subjects' Rights | adequate | The processor provides information on his website and in a fact sheet on the use of the BKMS® System in compliance with data protection rights that allow users to implement data subject´s rights and to react on consumer questions or e.g. dissents in data proceeding. The BKMS® System also provides a mailbox function that allows the sender of evidence to correct or delete his own personal data. |

# Experts' Statement

We affirm that the above-named IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Bremen, 2013-06-18 Dr. Irene Karper LLM.Eur.

| Place, date | Name of Legal Expert | Signature of Legal Expert |
|---|---|---|

Bremen, 2013-06-18 Ralf von Rahden

| Place, date | Name of Technical Expert | Signature of Technical Expert |
|---|---|---|

# Certification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

| | | |
|---|---|---|
| Kiel, | Independent Centre for Privacy Protection (ULD) Schleswig-Holstein | |
| Place, Date | Name of Certification Body | Signature |