Short Public Report on the IT-based service

BKMS® System

Recertification No. 1

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

IT-based service:	BKMS® System (Business Keeper Monitoring System).
Version:	3.1
Functional status:	April 2015.

2. Manufacturer or vendor of the IT product / 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: 2015/04/14 – 2015/05/28

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

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

5. **Certification** Authority**:**

Name: EuroPriSe Certification Authority
Address: Joseph-Schumpeter-Allee 25
53227 Bonn
Germany
eMail: contact@european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

The BKMS® System is a whistleblowing scheme, technically designed as a web-based application. It is available in three different configurations:

- BKMS® System as a central solution (collection, first verification and coordination of the incoming reports by a central department)
- BKMS® System as a decentral solution (reports are automatically forwarded to competent individual analysts by the system)
- BKMS® System as a solution for external experts (external experts deal with the first selection and the verification of the incoming reports).

These variants describe licence-related configurations of the BKMS® System and have been evaluated together as the BKMS® System.

A production system with a load balancer, four application servers and a database server, as well as a development and test system is part of the ToE.

7. General description of the IT product or IT-based service:

The BKMS® System facilitates the reporting of irregularities, hazards or risks. The system is used to support value management, compliance, or revision within an organisation. The BKMS® System allows a dialogue between whistleblowers and examiners (e.g. compliance officers, corruption agents, ombudsmen).

The BKMS® System is designed, maintained and operated in a high security data centre in Germany on behalf of the client by the Business Keeper AG as a software as a service (SaaS).

The BKMS® System can be customized to the needs of the user. Business Keeper AG makes the user (customer) aware of data protection requirements by means of, e.g., a privacy leaflet and trainings.

Because neither hardware nor software is delivered to the user, but a web-based service is made available, the BKMS® System is not an IT product, but an IT-based service.

Users of the BKMS® System are companies, organizations or public agencies. Examiners are usually employees of the user, such as compliance officers, or external experts chosen by the user, for example ombudsmen. Whistleblowers reporting about abuses, dangers or risks are typically citizens, employees or contractors.

The BKMS® System can be accessed through an https interface. The logon screen for examiners (August 2015) is available at https://client.bkms-system.net/bkwebanon/action/client/clientDisclaimer.do?language=ger. Usually, customers provide a link to the BKMS® System for potential whistleblowers on their websites. In addition, Business Keeper AG provides direct access links for whistleblowers to the BKMS® Systems of customers, who agreed to this publication, on its webpage under https://www.business-keeper.com/en/whistleblowing-system/for-whistleblowers.html.

Reporting

Whistleblowers can submit reports via a web form. They can choose between revealing their identity and acting anonymously or pseudonymously. Beyond that, they are given the opportunity to create a postbox, which can be used for a (pseudonymous) dialogue with the examiner.

The BKMS® System supports both reporting by name and anonymous / pseudonymous reporting. Business Keeper AG advises its customers in a leaflet on privacy, at system setup and in trainings to prefer reporting by name over anonymous / pseudonymous reporting.

In the context of the reporting, the whistleblower is provided with information on how to use the system. Depending on the requirements, customized privacy

statements or declarations of consent can be integrated into the respective webpage (e.g. in the case of transfer of personal data to locations outside of the EU).

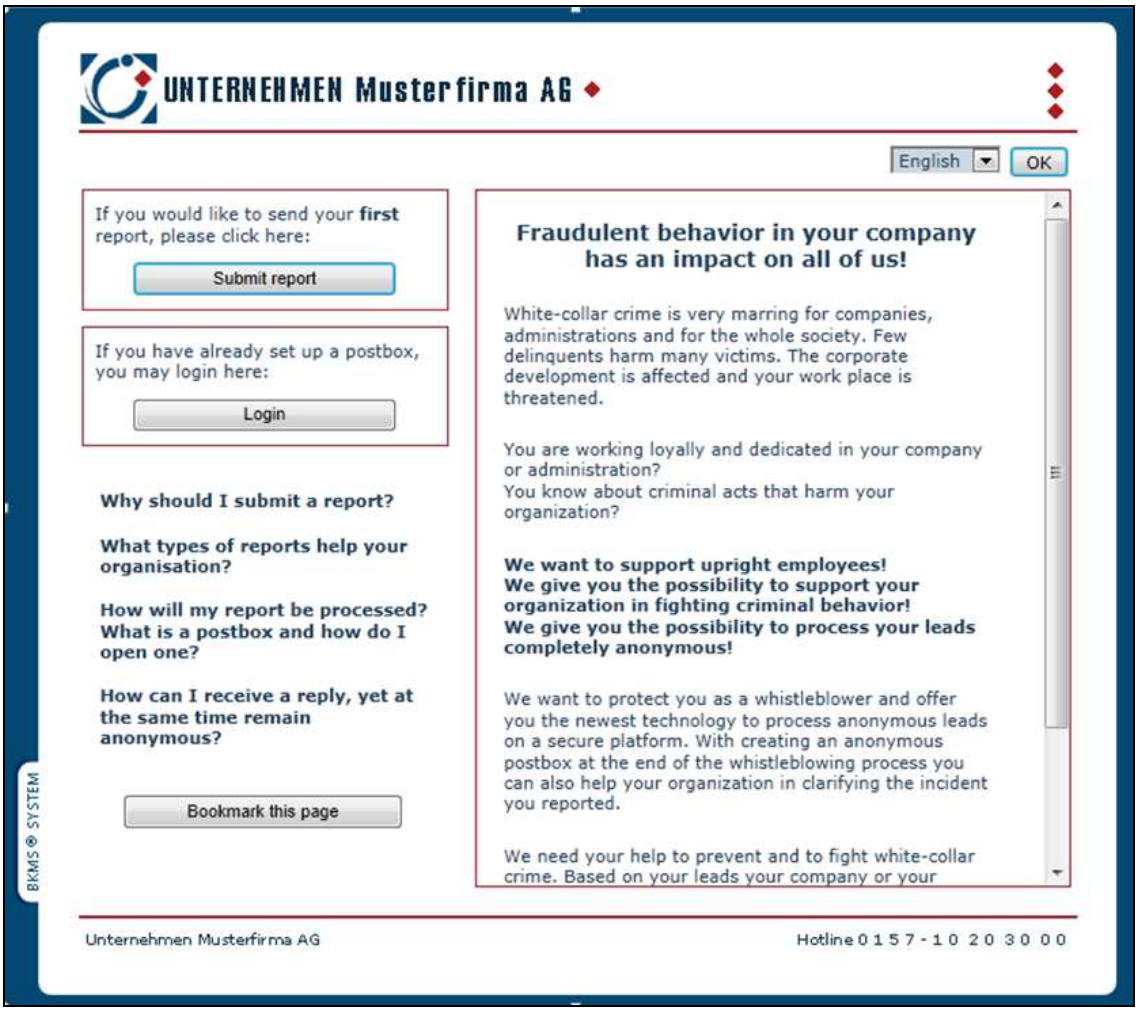

Figure 1: Part of the Test-User-Homepage of the BKMS® System

The whistleblower is then forwarded to a page dealing with certain reporting issues.

The specification of the reporting issues is carried out by the user on the basis of the applicable laws or regulations. Default reporting issues of the system particularly relate to certain types of crime (e.g., corruption and fraud). By contrast, they do not relate to violations against internal codes of ethics and codes of conduct, since here usually the interest of the company or organization

in processing the respective personal data is overridden by the interests for fundamental rights and freedoms of the data subjects concerned.

However, users may also select such reporting issues, but they are sensitized by a leaflet on privacy, by a document of account specification, as well as in training courses on the legal requirements.

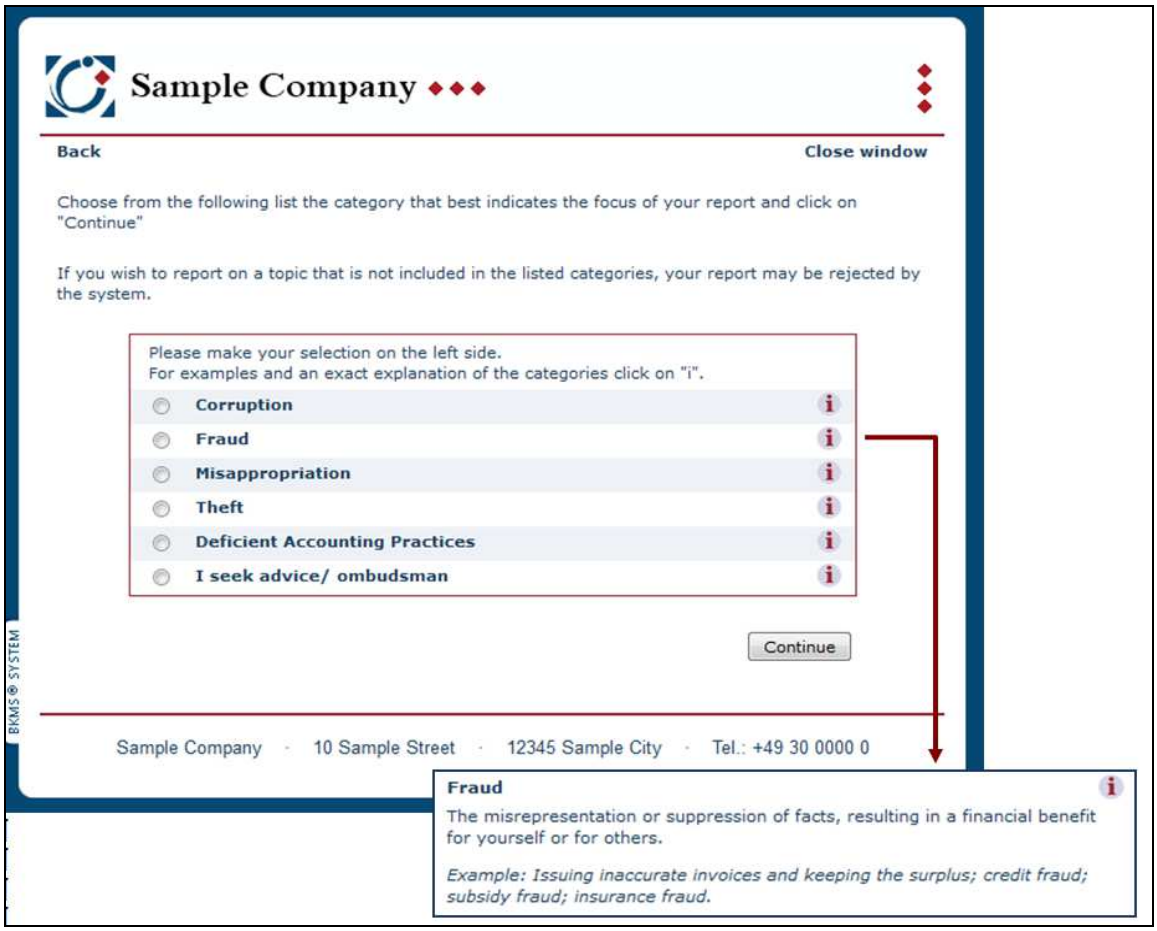

Figure 2 Reporting issues examples

After selecting one of the provided reporting issues, the whistleblower is asked to insert all relevant information on the incident and is also given the opportunity to upload relevant files.

Customers can define specific keywords indicating that a report is inadmissible (e.g. insults). Whenever such a term is used, the respective report is not accepted and this is being notified to the whistleblower.

After sending the report, a reference number is assigned to the report and displayed to the whistleblower. The report can also be printed.

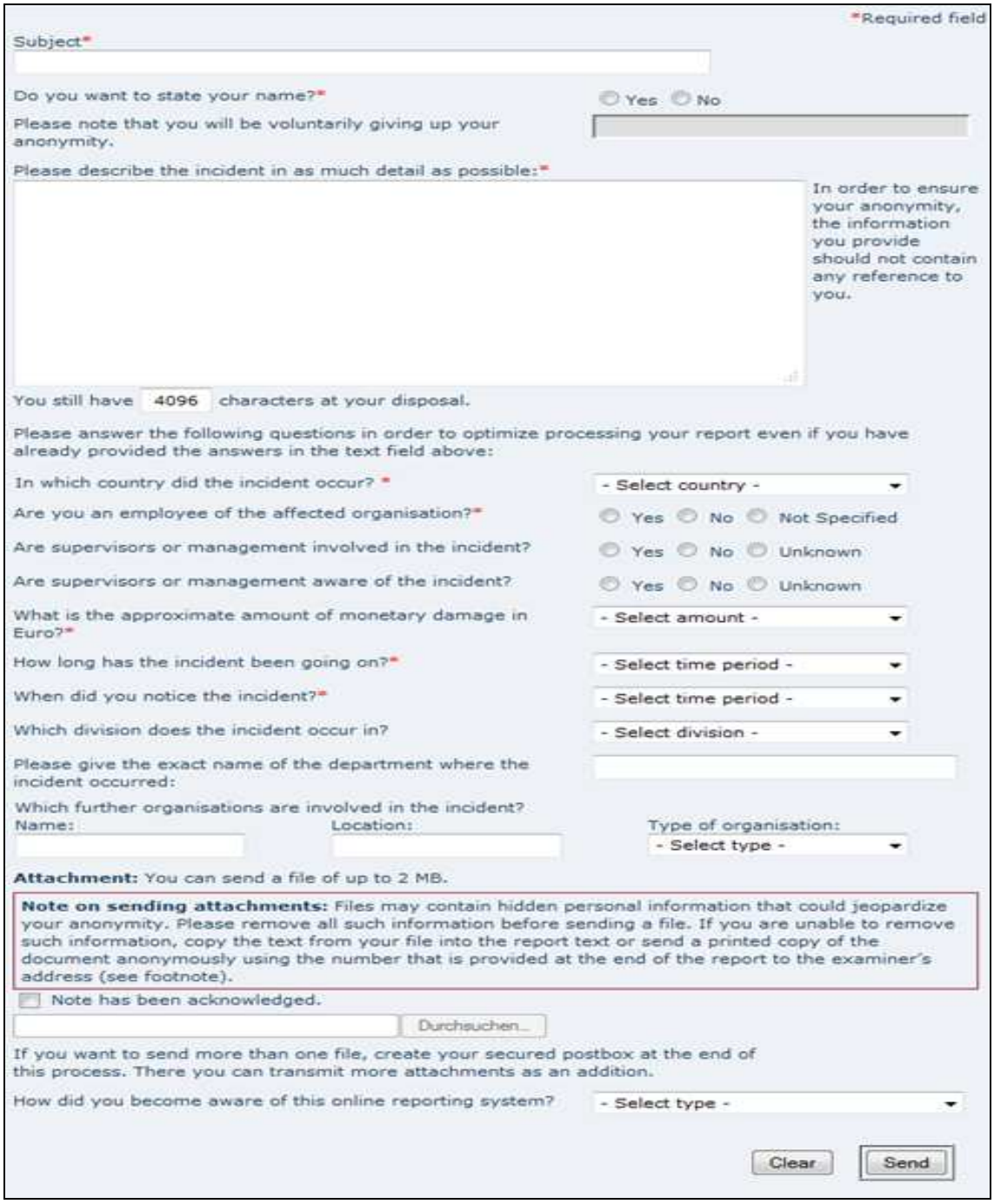

Figure 3: Whistleblower's data entry screen

Postbox

Only at this point, whistleblowers may set up a postbox, enabling them to conduct a dialogue with the examiner. They can choose a pseudonym as user name and a password. The password is stored as a hash. In the event of loss of access data there is no possibility to recover these credentials. The postbox is encrypted and assigned with a postbox ID. Whistleblowers receive information on the processing status and can send supplementing information via their postbox. They may read and print reports for a period of 42 days. The whistleblower's report in the database as well as the communication via postbox is encrypted using asymmetric encryption. This guarantees that only authorized persons have access to this data.

Examination of reports

Examiners must login to the system with user name and password. The password is stored as a hash value. Additionally a "DataPIN" is required for account activation and is used as an additional security feature for the assignment of permissions. After entering the DataPIN examiners have only access to those reports, for which they have been authorized. They receive an overview of the processing status and can handle them according to their granted rights.

Early warning system

The BKMS® System also includes an early warning system, which sends an SMS, e-mail or fax to selected persons (examiners) if certain key words appear in a report. The early warning system is intended to reduce the response time for specific risks. For this purpose, user ID and e-mail address as well as telephone or fax number of the authorized examiner are stored in the database.

Privacy Function

Examiners may make use of the so-called "privacy function" which enables them to make specific content of a report unrecognizable. Using this function means that personal information is blacked out or removed and thus no longer

visible to examiners handling the report. Only an examiner with the right to undo the privacy function can retrieve the original report.

Translation

Customers may decide to involve external translators for the purpose of translating reports. The function to include external translators is not covered by the standard scope of the BKMS® System and therefore has not been part of the evaluation. Customers are informed in the leaflet on privacy that external translators qualify as processors who process personal data on behalf of the controller (i.e. the customer of Business Keeper AG).

Data Analysis

The BKMS® System provides data analysis functionalities, such as log reports to evaluate the system access or standard reports with a non-personally identifiable analysis of reports. At the request of the user, individual reports can be configured. However, this is not part of the standard version of the BKMS® System and thus the evaluation.

Encryption

An asymmetric cryptosystem (public-key method) is used to encrypt the reports. The key pair is created on first usage by the customer and protected by a pass phrase. This ensures that the Business Keeper AG does not have access to the content of the reports. A report can only be decrypted by users inserting the DataPIN.

Archiving and Deleting

Reports can be deleted or archived by authorized examiners.

When a user is deleted, all respective rights are revoked. Name, first name and alias are preserved to prevent alias-duplicates and to preserve a revision-safe activity-log as a result.

Activity logs with the examiners' aliases are stored for 3 years in the default configuration of the BKMS® System. A shorter retention period of one year can be set on the user's request.

All (remaining) data is erased immediately upon termination of the contract between Business Keeper AG and the customer.

Administration of the BKMS® System

The BKMS® System provides three different roles: administrator, system administrator and user.

The role "administrator" allows for the editing of text modules to be used when processing submitted reports.

The true administrative role on the user's side is the system administrator ("Sysadm"). The system administrator grants or revokes access permissions and can set up, modify, or delete examiner (user) accounts, while s/he has no access to the content of the reports. The system administrator can scale access rights in the BKMS® System in detail.

The Business Keeper AG uses an SSH interface to access the servers of the BKMS® System for maintenance and backup purposes, and thereby has no reading access to the content of reports.

Responsible body and data processing on behalf

Customers of Business Keeper AG qualify as controller of the processing of personal data that results from the use of the BKMS® System.

When using the BKMS® System for external bodies, for example ombudsmen, they can be embedded in the workflow. Processing personal data, they qualify as controller if they decide about the review of a report to a greater extent. If such an external body receives personal data from the BKMS® System, then this constitutes a transmission in the meaning of EU data protection law which requires a legal basis.

Business Keeper AG qualifies as processor on behalf of the controller (i.e., their customer). It is to be highlighted that Business Keeper AG cannot access clear text, but only encrypted data.

Telekom Deutschland GmbH, which operates the data centre in Germany as a subcontractor, can also be qualified as a processor on behalf, although it does not have access to the reports in clear text as well.

Business Keeper AG has a contract template available which meets the demands of a controller – processor agreement as required by EU data protection law (cf. below at 11.1). Also, the subcontract between Business Keeper AG and Telekom Deutschland GmbH meets these requirements.

Scope of the certification

The target of evaluation (ToE) consists of the IT-based service BKMS® System (Business Keeper Monitoring System) v. 3.1.

The ToE does not cover:

- Special functionalities and configurations going beyond the standard version of the BKMS® System, especially the involvement of external translators, 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 the BKMS® System by Business Keeper AG
- the accounting processes between Business Keeper AG and their clients
- the IT environment of users and whistleblowers (hardware and software such as Internet browsers).

8. Transnational issues:

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

It is to be highlighted that currently a function is developed which makes the user aware of the issue of transfers of reports to examiners in third countries and supports the decision within the system. This function is still under development and not included in the current version of the BKMS® system, yet.

For the time being, Business Keeper AG provides guidance on how to comply with data protection requirements e.g. by means of a privacy leaflet and training courses for customers.

System and servers of the BKMS® System are located in a high security data centre within the Federal Republic of Germany.

9. Tools used by the manufacturer of the product / 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.

11. Modifications / Amendments of the IT product or IT-based service since the last (re)certification

The ToE version has changed from 2.7.3 to 3.1. With the exception of layout, hotfixes, patches and some internal organisational documents of Business Keeper AG nothing relevant with regard to the ToE has been added, nothing has been removed. SSLv3 has been turned off. The session key is now automatically changed. Freak-Prevention avoids the use of lower key standards. The connection of TOMCAT and database has been encrypted. Finally, the logo of Business Keeper AG has changed.

12. Changes in the legal and/or technical situation

None.

13. Evaluation results:

The following results were found within the framework of the audit:

13.1 Implementation of legal requirements

The relevant data protection framework on EU level consists of Directive 95/46/EC and Directive 2002/58/EC. These Directives have been implemented into national laws such as the German Federal Data Protection Act (BDSG) and the German Telemedia Act (TMG).

Furthermore, within EuroPriSe the opinions and working papers of the so-called Art. 29 Data Protection Working Party of the EU are to be considered. This coalition of the European Data Protection Authorities provided guidance 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”. Guidance on data protection issues concerning whistleblowing systems is also available on the national level (e.g., cf. 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”).

Customers of Business Keeper AG qualify as controller in the sense of EU data protection law. Thus, they are the ones who are responsible for a data protection compliant use of the BKMS® System. However, Business Keeper AG supports their customers by privacy-compliant default settings and an informative and comprehensible leaflet containing information on relevant data protection requirements. This privacy leaflet informs customers of Business Keeper AG of all requirements that are mentioned below:

A whistleblowing system is permissible if the processing of personal data is covered by a legal basis: The most relevant (potential) legal basis is Article 7(f) of Directive 95/46/EC which permits processing if it is necessary for the purposes of the legitimate interests pursued by the controller or by the third parties to whom the data are disclosed (if any), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects concerned.

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). However, usually not permissible are reports about violations of “soft facts” such as ethics or conduct regulations; these can only be justified exceptionally when no interests or fundamental rights of the data subjects stand in the way.

Processing of sensitive data requires one of the exceptions that are listed in Article 8(2) of Directive 95/46/EC (e.g., processing of personal data is legitimate if it is based on the data subject’s explicit consent). However, it has to be taken into account that such consent has to be freely given and can only be given by the data subject concerned. This means that the controller of a whistleblowing system cannot rely on consent as a legal basis for the processing of sensitive data in most of the cases.

Customers of Business Keeper AG may rely on the services of external examiners (third parties). In such a case, the disclosure of personal data to these third parties must be backed by a (separate) legal basis.

Companies which transfer personal 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 transfers to offices in third countries outside the EU and the EEA. Such a transfer is only legitimate if the respective third country provides an adequate level of data protection or if one of the derogations listed in Article 26 of Directive 95/46/EC applies: If the European Commission does not recognise an appropriate level of data protection in a third country, participation in the “Safe Harbour” programme (USA only), usage of one of the sets of standard contractual clauses that have been published by the European Commission or officially recognised binding corporate rules can also effect an appropriate level of data protection and privacy.

The requirements of Directive 2002/58/EC on cookies and the confidentiality of communications are covered by the BKMS® System. The web pages are encrypted via https and adequately protected against unauthorized reading of

communications during data transfer. Login functions require an appropriately secure password. The data encryption of reports and communications ensures confidentiality (cf. Article 5(1) of Directive 2002/58/EC).

A session cookie is placed on the terminal of an examiner who logs into the BKMS® System in order to maintain the session. The user is informed about this on the webpage “Data privacy and data security in the BKMS® System”. The consent requirement according to Article 5(3) of Directive 2002/58/EC as amended by Directive 2009/136/EC is not applicable, since the session cookie “is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service” (cf. Art. 5(3), 2nd sentence, 2nd alternative).

13.2 Data avoidance

The BKMS® System facilitates the anonymisation or pseudonymisation of personal data by means of a special “privacy function”: An examiner may specify personal data such as names or unique identifiers that are part of a report. The application of the privacy functionality results in the blacking of the specified data (making them unreadable). Only an examiner with the right to undo the privacy functionality is able to retrieve the original report.

Secondary data - such as log files – are automatically deleted after 3 years using the default configuration of the BKMS® System. A deviating retention period of one year can be set on the user's request. In addition, the BKMS® System provides functionalities to avoid or minimize the processing of personal information, such as a differentiated authorization concept; access to personal data within the BKMS® System can thus be limited to a need-to-know-basis.

13.3 Transparency

A privacy leaflet informs the data controller and its employees (examiner) about all relevant data protection requirements (cf. already above at 11.1). In respect of transparency, it reminds customers of Business Keeper AG of their duty to inform (potential) whistleblowers in accordance with Article 10 of Directive

95/46/EC and to inform persons who are accused in a whistleblowing report in accordance with Article 11 of Directive 95/46/EC.

13.3 Data security

The servers are operated in a data centre with strong access controls (physical and logical). All data transfers within the BKMS® System are secured via SSL. Also, a backup policy is in place ensuring the appropriate backup of data.

Furthermore, all information provided by the whistleblower is encrypted and not accessible by the data processor or other unauthorized persons. The used software module is protected against manipulations by means of a hash value.

13.4 Data subject rights

Business Keeper AG provides information on their website and in a privacy leaflet on how to use the BKMS® System in compliance with data protection law, especially how to implement processes dealing with data subject rights and how to react on consumer requests. The BKMS® System also provides a postbox functionality that gives the whistleblower the opportunity to provide additional information at a later point in time.

14. Data flow:

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

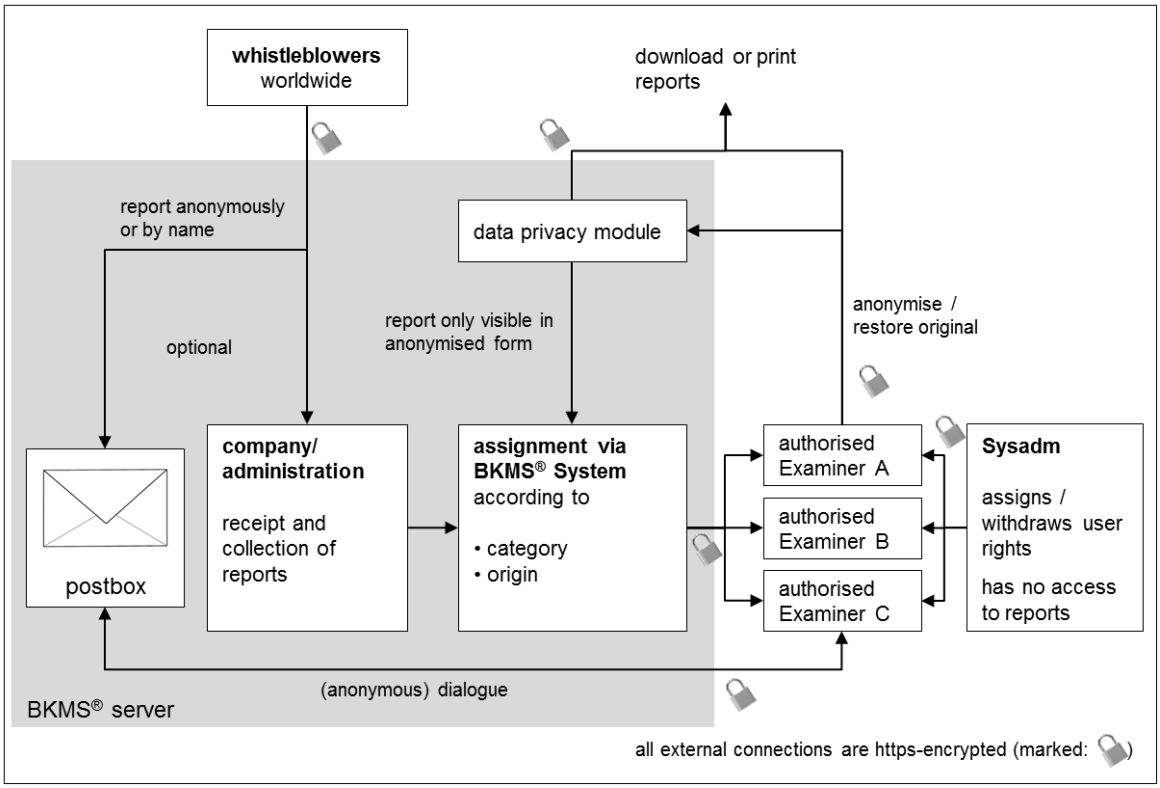

Figure 4: data flow

15. Privacy enhancing functionalities:

In the BKMS® System the confidentiality of personal data is ensured by an authorization concept that enables very fine-grained access rights.

The provided service description and the information about the data processing are particularly transparent and they support the implementation of the data subject rights in an optimal manner.

Organizational and technical measures implemented by the data processor/s to ensure data security and privacy go beyond the legal requirements:

- The data controller is very well informed about compliance by Business Keeper AG by means of a leaflet dealing with privacy aspects.
- The data centre housing the BKMS® System components is a highly secured data centre.

16. Issues demanding special user attention:

None

17. Compensation of weaknesses:

There are no requirements assessed as “barely passing” for the BKMS® System.

Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	adequate	Customers are well informed about the privacy principle of data avoidance and minimisation by the Business Keeper AG by means of a privacy leaflet. Furthermore, the BKMS® System allows to make personal data unrecognizable by using the special “privacy function”.
Transparency	adequate - excellent	Documentation and privacy leaflet are informative, up-to date and understandable; Business Keeper AG also provides a security policy and a privacy concept. Information on the website of Business Keeper AG dealing with data protection complies with the relevant legal framework.
Technical-Organisational Measures	excellent	Organizational and technical measures on data security and privacy are above legal standards. The data centre is located in Germany and meets all high level requirements regarding (e.g.) physical access control, recovery mechanisms as well as network and transport security. 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	Business Keeper AG provides information on how to implement processes dealing with data subject rights and how to react on consumer requests in the privacy leaflet. The BKMS® System also provides a postbox functionality that enables whistleblowers to provide additional information at a later point in time.

Experts' Statement

We affirm that the above-named IT product / 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, 2015-08-01 Dr. Irene Karper LLM.Eur.

Place, date	Name of Legal Expert	Signature of Legal Expert

Bremen, 2015-08-01 Ralf von Rahden

Place, date	Name of Technical Expert	Signature of Technical Expert

Recertification 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.

Bonn,	EuroPriSe Certification Authority	
Place, Date	Name of Certification Body	Signature