Short Public Report

BKMS® Compliance System

Recertification No. 3

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

BKMS® Compliance System is an IT-based service with a functional status from February 2020. It is a collective name for certain modules of the Compliance System ("BKMS® Compliance Platform") running on a BKMS® server. The well-known BKMS® system (version 3.1., unchanged), already certified according to EuroPriSe, is the core of the web-based system. In addition, the following extensions are covered by this recertification for the first time:

- BKMS® VoiceIntake and BKMS® Translation as extensions to BKMS® System, v. 3.1,

- BKMS® Case Management, v.3.1,

- BKMS® Third Party, v.1 and

- BKMS® Business Approvals, v.1

Since the user is provided neither with hardware nor with software, but rather with a data processing service in the web-based BKMS® Compliance System, the ToE is not an IT product, but an IT-based service.

2. Manufacturer or vendor of the IT-based service:

Company Name:	Business Keeper AG
Address:	Bayreuther Straße 35, 10789 Berlin, Germany Web: www.business-keeper.com
Contact Person:	Mr. Lennart Hock, Privacy Officer, Business Keeper AG

3. Time frame of evaluation:

2019/11/21 – 2020/05/04

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

Name of the Legal Expert:	Mrs. Alisha Gühr
Address of the Legal Expert:	datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen, Germany aguehr@datenschutz-cert.de
Name of the Technical Expert:	Dr. Irene Karper
Address of the Technical Expert:	datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen, Germany ikarper@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® Compliance System enables the processing and administration of compliance processes. BKMS® system is the core of the BKMS® Compliance System. IT enables a dialogue between whistleblowers and examiners (e.g. compliance officers, corruption agents, ombudsmen) in order to report irregularities, dangers or risks. It is used to support value management, compliance or auditing. The customer can also make use of the extensions BKMS® VoiceIntake, BKMS® Case Management, BKMS® Third Party and BKMS® Business Approvals. They build on the data processing processes of the BKMS® System environment. With VoiceIntake, for example, voice messages of whistleblowers can be recorded in the BKMS® system. BKMS® System also has the function to translate notes and answers within the system

with the help of a translation agency chosen and commissioned by the user (BKMS® Translation). BKMS® Case Management allows for the management of compliance relevant messages in a case system. BKMS® Third Party is used in the context of compliance for risk management and the review of supplier relationships. With BKMS® Business Approvals, mandatory information and approval processes can be documented in an audit-proof way, e.g. when implementing gift acceptance guidelines.

Users of the BKMS® Compliance System are companies, organizations or public agencies. Examiners are usually employees of the user, such as compliance officers, or external experts chosen and commissioned by the user, for example ombudsmen. Whistleblowers reporting about abuses, dangers or risks are typically citizens, employees or contractors. BKMS® Compliance System is developed by Business Keeper AG as Software as a Service (SaaS) and provided by Business Keeper as a processor on behalf of the user. The service is maintained and operated in data centers in Germany and Switzerland.

The ToE includes a production system, load balancer, four application servers, a database server, and a development and test system.

The ToE does not include the user's operating environment and specific configurations of BKMS® Compliance System and its components at the user's site, in particular

- the creation or use of individual reports (BKMS® System)

- the establishment or use of topics for reports (BKMS® System)

- the installation or use of information texts or declarations of consent in the context of the submission of reports (BKMS® System)

- BKMS® Translation in combination with the translation agency contractually bound to Business Keeper AG

- The optional configuration of an automatic voice distortion for BKMS® VoiceIntake by Business Keeper AG

- use of the Alert Manager function and the Dow Jones Risk & Compliance watch list within BKMS® Third Party

- use of the function for integrating search engines in BKMS® Third Party

- integration of user-specific questionnaires and self-disclosure forms in BKMS® Third Party and their subsequent use

Furthermore, the ToE does not include the licensing and sales processes at Business Keeper AG, apps for tablets or smartphones or further services or consulting by Business Keeper AG.

7. General description of the IT-based service:

The BKMS® Compliance System can be accessed through an https interface.

BKMS® System

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 informs its customers in a leaflet on privacy, at system setup and in trainings about reporting by name or 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). However, customized documents / texts are as such not part of the ToE of this recertification.

A whistleblower who wants to submit a web-based report must open a customer specific webpage (front page) that may look as follows:

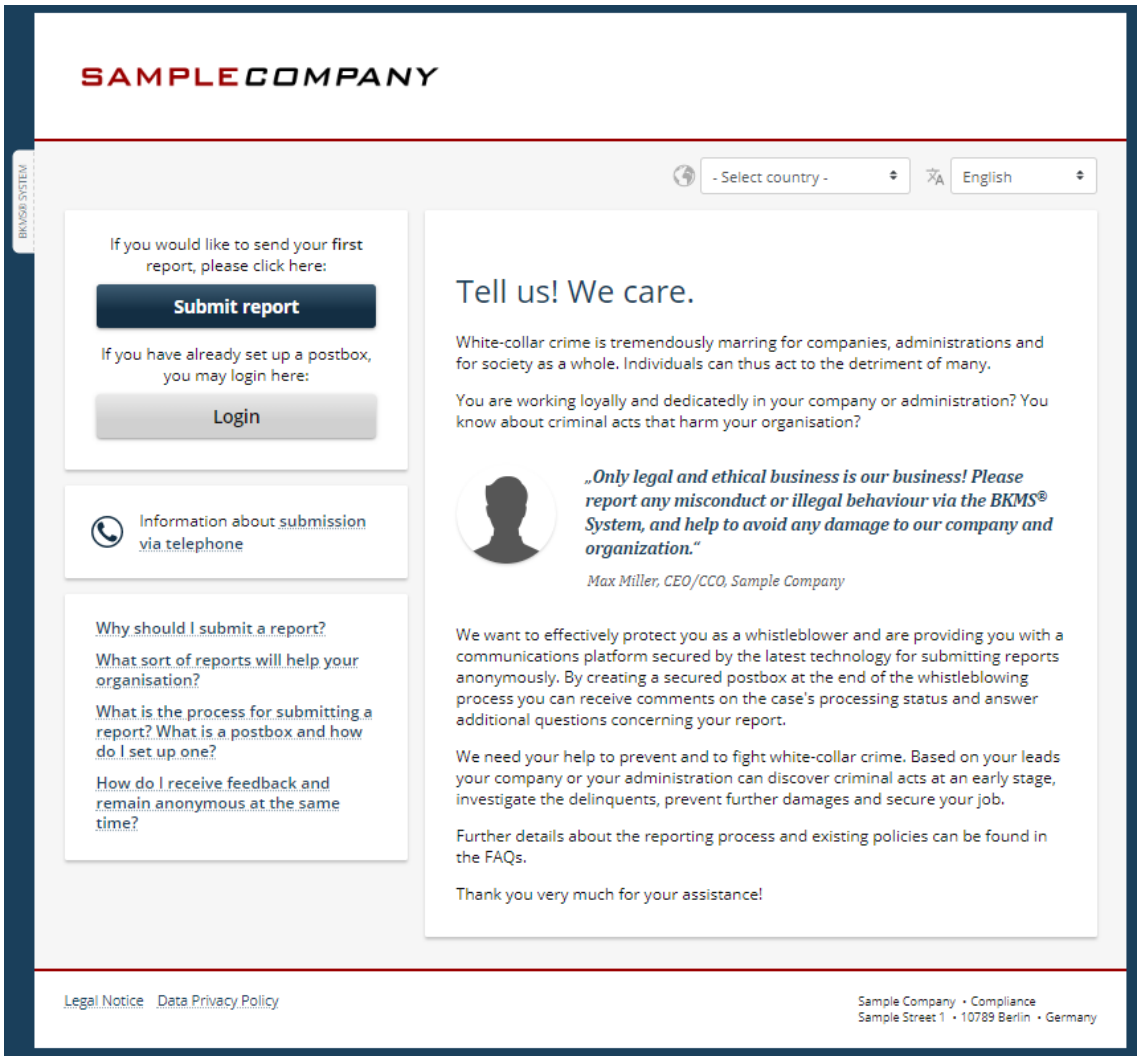

Figure 1: Part of the Test-User-Homepage of the BKMS® System

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 select such reporting issues nevertheless, but they are sensitized in a leaflet on privacy, in a document providing insights on possible account specifications, as well as in training courses on the legal requirements that they must meet in such a case.

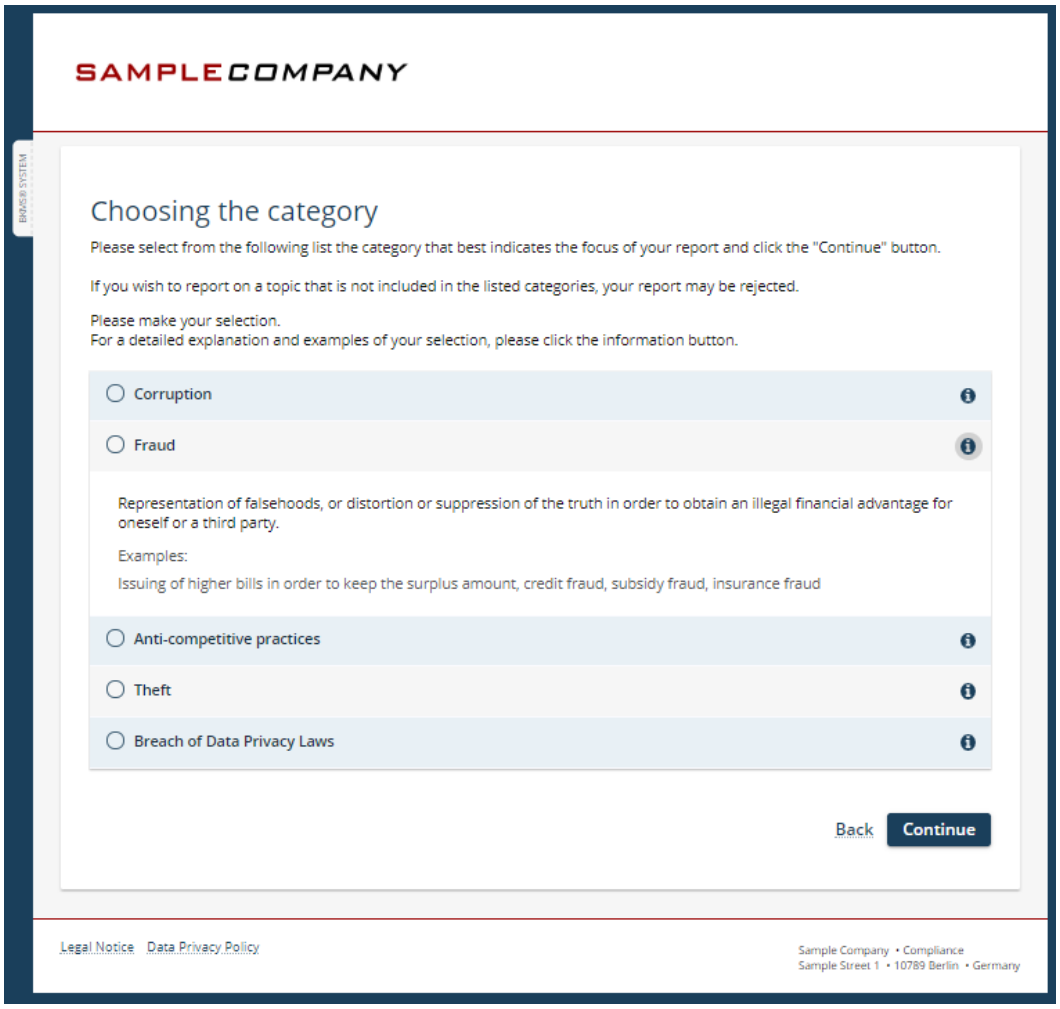

Figure 2: Reporting issues examples

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.

SAMPLECOMPANY

BKMS® SYSTEM

Report to be sent to: Sample Company, Berlin

Category: Fraud

* Required field

*Subject:

*Do you want to state your name?

- Yes
- No

*Please describe the incident in as much detail as possible:

If you would like to stay anonymous, you will be protected by the BKMS® technology. Please make sure that the information you provide does not contain any reference to you.

0/5000

Please answer the following questions in order to optimise the processing of your report even if you have already provided the answers in the text field above:

*Which country is affected?

- Please select -

*In which division did the incident occur?

- Please select -

Are you an employee of the affected organisation?

- Yes
- No
- Not specified

Have you already informed anyone else about the incident?

- Yes
- No

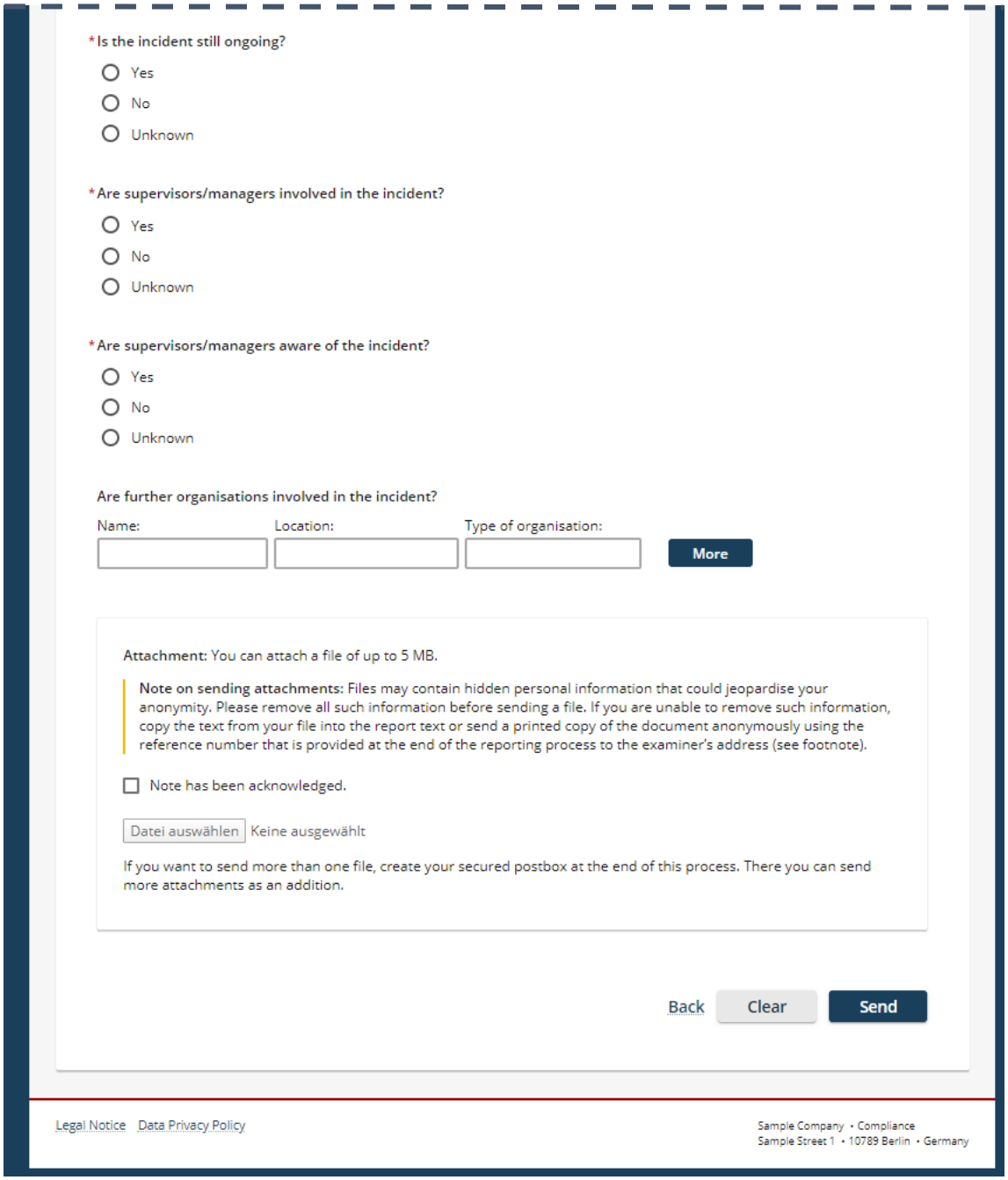

Figure 3: Example of data entry screen for whistleblowers

Postbox

Only at this point, whistleblowers may set up a postbox, enabling them to enter into 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 a loss of these access data there is no possibility to recover the 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 authorised 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 authorised. They receive an overview of the processing status and can handle reports according to their granted rights. The "Examiner DataPIN" allows an individual assignment (compared to the common DataPIN for all examiners), thus minimizing the risk of misuse by unauthorised persons. When an employee leaves the company, only the user profile of this examiner has to be deactivated and deleted.

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, the user ID and e-mail address as well as the telephone or fax number of the authorised examiner are stored in the database.

Privacy Function

Examiners may make use of the so-called "data privacy function", which enables them to render 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

There is also the possibility to forward reports or replies to reports via the BKMS® system to translation agencies designated and commissioned by the user. For this purpose, the examiner releases the text to be translated to the external translator within the BKMS® System. For this purpose, BKMS® System provides a specific user role ("external translator"). The translated text is communicated within the BKMS® System, translated in a mask, and forwarded

back to the examiner. This function is now covered by this recertification for the first time. External translators process reports and replies to reports as processors on behalf of the users (customers) of the BKMS® System. They are freely selected and commissioned by the users and are subject to their instructions. BKMS® Translation in combination with the translation agency bound to Business Keeper AG is not part of the ToE of this recertification.

Auditor

Another specific user type ("auditor") is available, too. An auditor receives read-only rights to user-defined areas, e.g. to the activity log, audit log, or user administration. The auditor has no access to reports. The areas are enabled by the Sysadm of the customer (short for: system administrator).

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 not covered by this recertification.

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 only be deleted by an authorised examiner after the case has been closed and commented on.

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. Deleted users are still displayed to the Sysadm for revision purposes. It is planned that in the future, information about a user will be deleted three years after his last activity. Since this has not yet been implemented technically, Business Keeper AG recommends to its customers that the Sysadm edits the user's data before deletion (surname and first name

are replaced by aliases, e.g.). The alias, on the other hand, cannot be adjusted and is still displayed to the Sysadm (since activities are still assigned to users in messages using aliases).

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

Concerning the administration of the BKMS® System, three different roles are to be distinguished:

The role "administrator" allows for the editing of text modules to be used when processing submitted reports. It is granted to users on the customer's side.

The true administrative role on the user's / customer's side is the 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. The respective employees of Business Keeper cannot access the content of reports.

BKMS® VoiceIntake and BKMS® Translation

BKMS® VoiceIntake complements the BKMS® System with the possibility to submit reports by telephone. In principle, reports submitted by telephone are processed in the same way as reports given electronically via the web-based interface. BKMS® VoiceIntake acts like an answering machine on which whistleblowers may leave messages. First, the user must call a specific phone number. S/he is then required to listen to an announcement recorded by the user / customer informing whistleblowers about the functioning of BKMS® VoiceIntake, providing them with relevant data protection information and usually asking them for their consent to the processing of their personal data. The whistleblower may consent, e.g., by answering with "yes" to a corresponding question such as "do you consent?". S/he can then record a message and answer to specific questions (usually the same ones as in the web-based scenario). Finally, the whistlelbower can create a "telephone

postbox". In return, the examiner can reply to the whistleblower by recording messages and leaving them in the "telephone postbox" for the whistleblower.

Audio messages received via BKMS® VoiceIntake are transmitted to the BKMS® System. However, it is important to note that telephone numbers of whistleblowers are not recorded and forwarded to the BKMS® System. The competent examiner then listens to the message and transcribes it. Both the audio message and its transcription are stored in the BKMS® System. Customers are advised that information contained in the audio messages, which is obviously not necessary, should not form part of the transcription of the message or should subsequently be blacked out. In such a case, the audio message should be deleted immediately after the transcription.

BKMS® Case Management

BKMS® Case Management provides customers with additional functionalities for compliance case management and documentation. It serves the documented examination of the facts related to a report and the implementation of possible follow-up measures. While basic report processing and case management functionality is already integrated into the BKMS® System, BKMS® Case Management offers expanded management options that make it possible to satisfy specific standards and regulatory requirements.

Reports from the BKMS® system can be transferred as a new case to BKMS® Case Management. In addition, the management of financial fraud or the Critical Incident Reporting System (CIRS) is possible. Since personal data may be named in the cases (victims, perpetrators, involved parties, witnesses), the case management is structured in such a way that pseudonyms can be used to identify persons.

BKMS® Third Party

BKMS® Third Party can be used independently from the other applications in the BKMS® Compliance System. It enables organizations a structured, uniform and documented review and approval process of business partners ("Third Party Due Diligence"). The BKMS® Third Party is used with the aim to identify risks in a documented way before working with new business partners and thus to avert potential damage to the organisation. It can be stored in the system whether personal data was collected with the consent of the respective data subject.

Authorised employees ("Applicant") can create requests to check new business partners. (Potentially personal) data about the business partner and personal

data about the user / applicant (access data, log data) is processed within BKMS® Third Party. Business partner data is usually business-related data that does not relate to a natural person, since it is used to evaluate the business partner or vendor. However, it cannot be ruled out that, for example, in the case of sole traders, the data may relate to a natural person and thus may be personal data.

The purpose of BKMS® Third Party is to support customers with approval processes relating to new business partners. Theoretically, this extension could be used for applicant or employee screening as well. In terms of data protection law, this would be critical (cf. No. 16 below). However, this would not be in line with the purpose or BKMS Third Party® and such a use is thus not covered by the recertification according to EuroPriSe.

Optionally, specially authorised users (Alert Manager) can use the external data source of the Dow Jones Risk & Compliance watch list, which can be queried and displayed via BKMS® Case Management. This is not part of the ToE. Also optional is the function that within the examination process, a search is carried out via the Internet. It is also not part of the ToE (cf. No. 16 below).

The user is sensitized in the privacy leaflet, e.g. not to make automated individual case decisions and to document weighing decisions in the comment field for reasons of transparency.

BKMS® Business Approvals

BKMS® Business Approvals can be used independently from the other applications in the BKMS® Compliance System. It supports mandatory information and approval processes. Services and processes can be applied for, evaluated and approved or denied based on the guidelines specified by the user, such as when granting or accepting gifts for employees or in the context of sponsoring. The approval process is documented in the system. Once again, the main objective is to support the compliance processes and, for example, prevent corruption. Safety levels are defined for the services and processes (low risk, medium risk, high risk). The user defines the security levels according to his needs. Depending on the security level, the case is then assigned to a manager of the corresponding security level in the company or, in the principle of multiple control, to different managers.

8. Transnational issues:

Since the BKMS® Compliance System is a web-based application it can be used worldwide. Organizations deploy the BKMS® Compliance System at their branches within the EU, the EEA or worldwide. 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® Compliance System are located on customers request in high security data centers either located in Germany or in Switzerland.

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 January 2017.

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

The BKMS® System was extended by the above-mentioned modules. The extended solution is now trademarked as BKMS® Compliance System. Relevant documents within the ToE, like the privacy leaflet or the sample controller – processor agreement, some documents of the ISO/IEC 27001-certified ISMS and other auditing or test documentation were updated.

12. Changes in the legal and/or technical situation

Worldwide there are many regulations on compliance and whistleblowing matters, which are subject to constant change. Worth mentioning is Directive (EU) 2016/943 on the protection of confidential know-how and confidential business information (trade secrets) against illegal acquisition, use and disclosure. It protects trade secrets, but neither imposes penalties on whistleblowers nor prohibits data collection in whistleblowing systems. Recital 20 states that "the measures, procedures and remedies provided for in this Directive should not be used to restrict whistleblowing activities". It should be stressed that these provisions do not constitute a data protection basis for data

processing within the meaning of the GDPR or national data protection provisions.

Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law is also applicable in the context of infringements of Union law. Essential requirements in terms of data protection are contained in Art. 17 and Art. 6 of the Directive. According to Article 17(2), personal data, which are manifestly not relevant for the handling of a specific report, shall not be collected or, if accidentally collected, shall be deleted without undue delay. This corresponds to the principle of data minimisation. Article 6(2) provides that, without prejudice to existing obligations to provide for anonymous reporting by virtue of Union law, this Directive does not affect the power of Member States to decide whether legal entities in the private or public sector and competent authorities are required to accept and follow up on anonymous reports of breaches. EU Member States may therefore provide for other rules concerning the anonymity of whistleblowers. Implementing legislation for this directive is to be passed by 17.12.2021. The interaction of this Directive with the data protection requirements of the GDPR and, if applicable, national regulations will only then need to be considered in more detail.

A paradigm shift has taken place since the last EuroPriSe certification with regard to the previously held opinion that anonymous reporting should not be the rule. Whereas in 2006 the Art. 29 Data Protection Working Party still took the view that anonymous reports were only desirable in exceptional cases to protect against abusive reporting, supervisory authorities are now increasingly turning away from this view. In many EU member states, reporting by name is no longer required, but rather the confidentiality of whistleblower systems is now the focus. In France and Spain, for example, named and anonymous reports are legally equal and confidentiality is required. The German DSK even goes one step further and explicitly recommends anonymous reports.

Finally, it should be mentioned that the German legislator introduced a new provision (Section 29(1) sentence 1) to the Federal Data Protection Act in the course of this act's adaption to the GDPR. This provision allows for exceptions from the duty to inform pursuant to Art. 14 GDPR under certain circumstances. In the whistleblowing context, this provision may provide for greater protection of the identities of whistleblowers who had reasonable grounds to believe that the information on breaches they reported was true at the time of reporting.

Audit and approval processes in BKMS® Third Party and Business Approvals may be based on the fulfilment of a legal obligation within the meaning of Art.6 para. 1 lit. c GDPR, for example, when it comes to the conclusion of contracts with business partners for whom recording, storage or archiving obligations exist. Such obligations may be derived from commercial, trade, tax or social law. Other examples are the German Money Laundering Act (Sections 10, 11a), the French Loi sur le blanchiment d'argent (Art. 3) or the Spanish Ley de prevención del blanqueo de capitales y de la financiación del terrorismo (Art. 3) as well as other specific legal provisions requiring business partner identification / verification (e.g. Regulations (EC) 881/2002 and (EC) 2580/2001).

13. Evaluation results:

The following results were found within the framework of the legal and technical evaluation:

Implementation of legal requirements

General legal requirements for all modules of the BKMS® Compliance System

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

When using the BKMS® Compliance 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 has access to personal data in the BKMS® Compliance 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. The data centers, which are located in Germany or in Switzerland, can also be qualified as processors ("another processor"), although they do 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 (Customer – Business Keeper AG) agreement as required by EU data protection law. The sub-contracts between Business Keeper AG and the data centers meet these legal requirements, too.

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 about best practices.

Legal requirements for whistleblowing systems

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 Art. 6 (1) lit. f GDPR: Processing of personal data shall be permitted where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

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 factors). However, usually not permissible are reports about violations of "soft factors" such as ethical rules or does of conduct; 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 9 GDPR (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.

In addition, there are scattered, often sector-specific regulations in the individual Member States. In Germany, for example, Section 25a (1) sentence 6 no. 3 KWG (for credit institutions) and Section 23 (6) VAG (for insurance companies) are worthy of mention. In France, for example, Art. 8 para. 3 Sapin II applies.

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 may be legitimate if the respective third country provides an adequate level of data protection: If the European Commission does not recognise an appropriate level of data protection in a third country, participation in the "Privacy Shield" 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 at this time.

Further legal requirements for all / some modules of the BKMS® Compliance System

Data processing in all modules of the BKMS® Compliance System is carried out for the purpose of protecting the company from economic damage, criminal offences or loss of reputation. There is therefore a legitimate interest in the processing of personal data about, e.g., suppliers or employees in accordance with Art. 6 para. 1 lit. f GDPR. The persons concerned must be given the opportunity to object on grounds relating to their particular situations.

In exceptional cases, data processing may also be based on revocable consent pursuant to Art. 6 para. 1 lit. a GDPR, provided that such consent can be effectively obtained. In the context of employment relationships, however, consent is generally not voluntary.

Examination and approval processes in BKMS® Third Party and Business Approvals may also be based on the fulfilment of a legal obligation within the meaning of Art.6 para. 1 lit. c GDPR, for example in the case of the conclusion of contracts with business partners for which recording, storage or archiving obligations exist. Such obligations may be derived from commercial, trade, tax or social law. Other examples for relevant legal obligations are the German Money Laundering Act (§ 10, 11a), the French Loi sur le blanchiment d'argent (Art. 3) or the Spanish Ley de prevención del blanqueo de capitales y de la financiación del terrorismo (Art. 3) as well as other specific legal provisions requiring business partner identification / verification (e.g. Regulations (EC) 881/2002 and (EC) 2580/2001).

Art. 88 GDPR is particularly relevant for the processing of employee data. This opening clause allows member states to regulate the protection of employee

data. E.g., the German legislator has made use of this opportunity (cf. Section 26 FDPA). Collective regulations can also be considered as a legal basis (cf. also Recital 155 GDPR).

When processing personal data using the BKMS® Compliance System, the regulations of Art. 10 GDPR must be observed.

The requirements of Directive 2002/58/EC on cookies and the confidentiality of communications are met. The web pages are encrypted via https and adequately protected against unauthorised reading of communications during data transfer. Login functions require an appropriately secure password. The 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).

Data avoidance

The BKMS® Compliance System facilitates the anonymisation or pseudonymisation of personal data by means of a special "data 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 blackening 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. A deviating retention period of one year can be set on the user's request. In addition, the BKMS® Compliance System provides functionalities to avoid or minimize the processing of personal information, such as a differentiated authorization concept; access to personal data within the System can thus be limited to a need-to-know-basis.

Transparency

A privacy leaflet informs the customer / controller and its employees about all relevant data protection requirements. Amongst others, it reminds customers of

their duty to inform data subjects in accordance with Articles 12, 13 and 14 GDPR.

Data security

The data centers in Germany and Switzerland, where the components of BKMS® Compliance System are available at the customer's request, demonstrate a high degree of physical safety and are all certified according to ISO/IEC 27001. The servers are managed with very high access controls and high availability. Data transfers are secured via SSL. An adequate backup concept as well as a contingency plan support availability.

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

The Information Security Management System of Business Keeper AG with the scope "Secure operation of the BKMS® Compliance System" is certified according to ISO/IEC 27001 (Certificate-ID: DSC.501.11.2017, Date of expiry 22.11.2020).

Data subject rights

Business Keeper AG provides information on their website and in a privacy leaflet on how to use the BKMS® Compliance System in compliance with data protection law, especially how to implement processes dealing with data subject rights and how to react on data subject requests.

14. Data flow:

Four models of data flow are presented below.

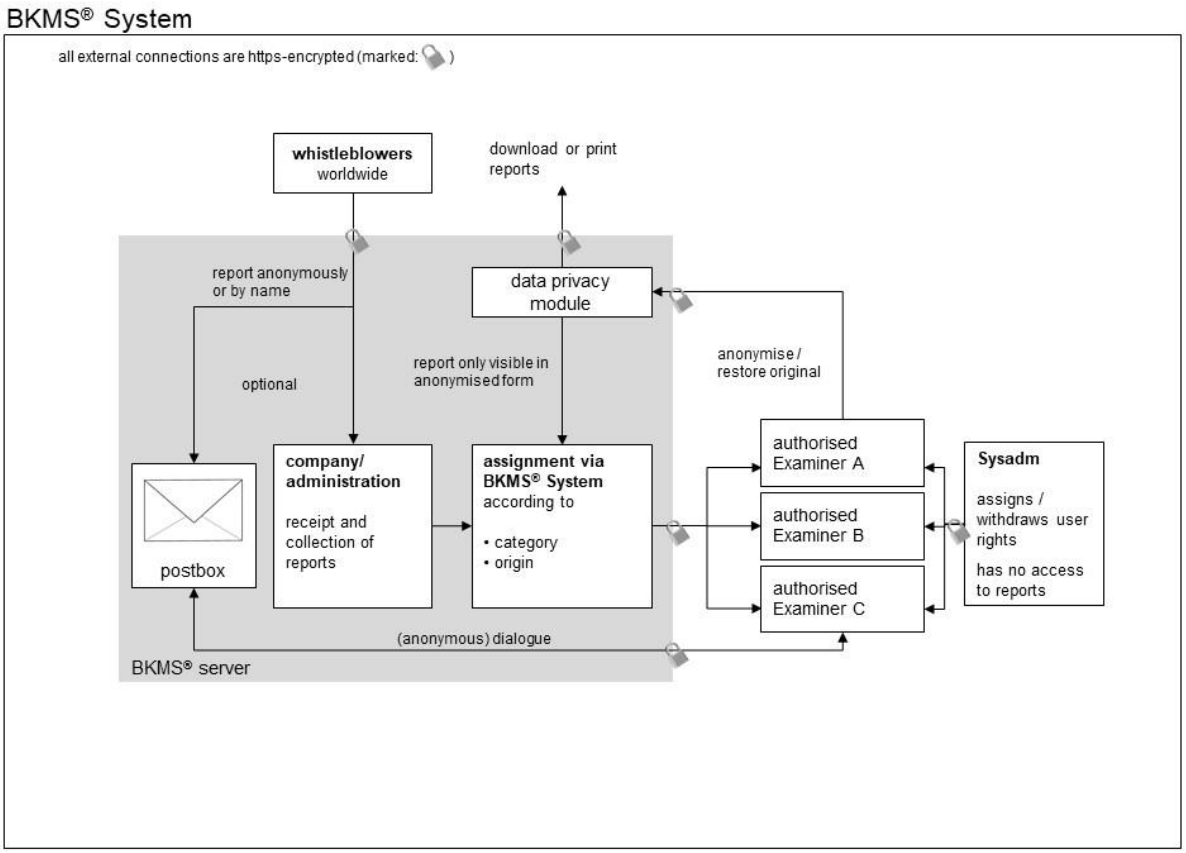

Figure 4: Data flow BKMS® System with VoiceIntake und Translation

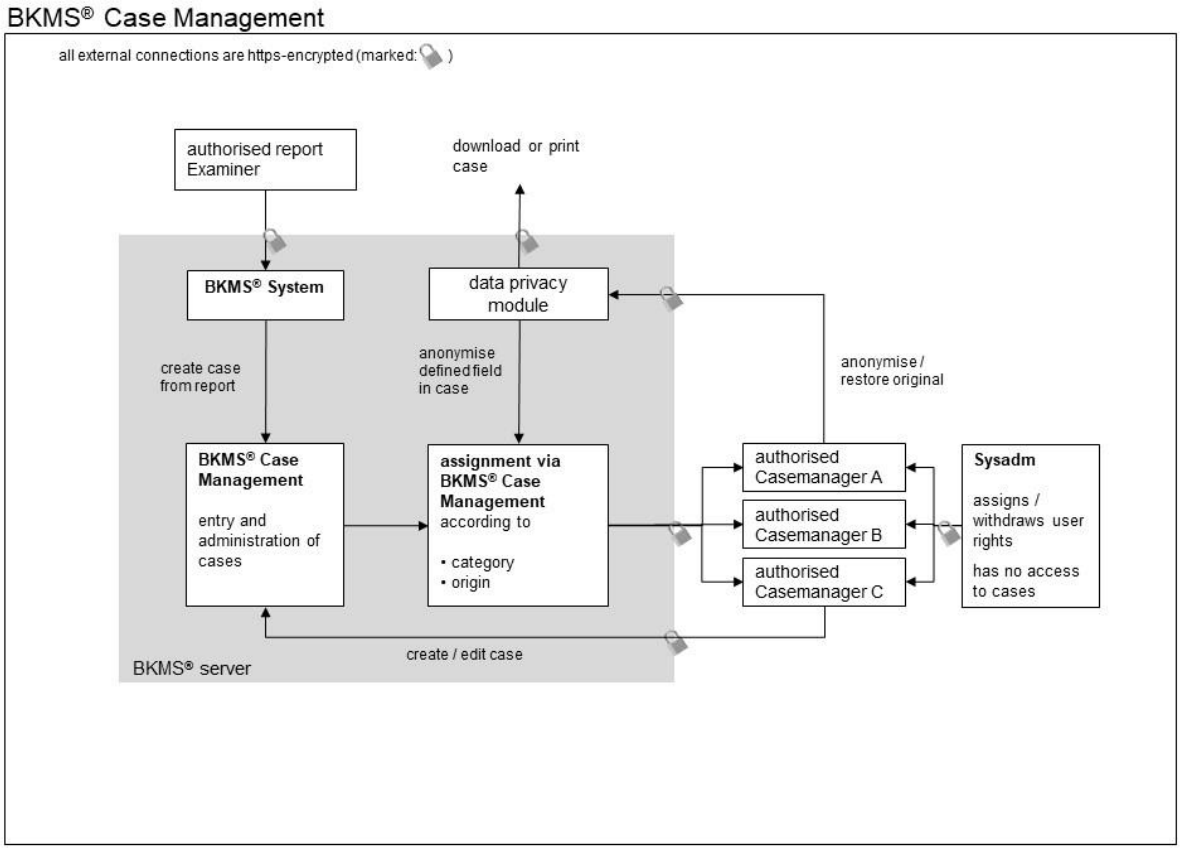

Figure 5: Data flow BKMS® Case Management

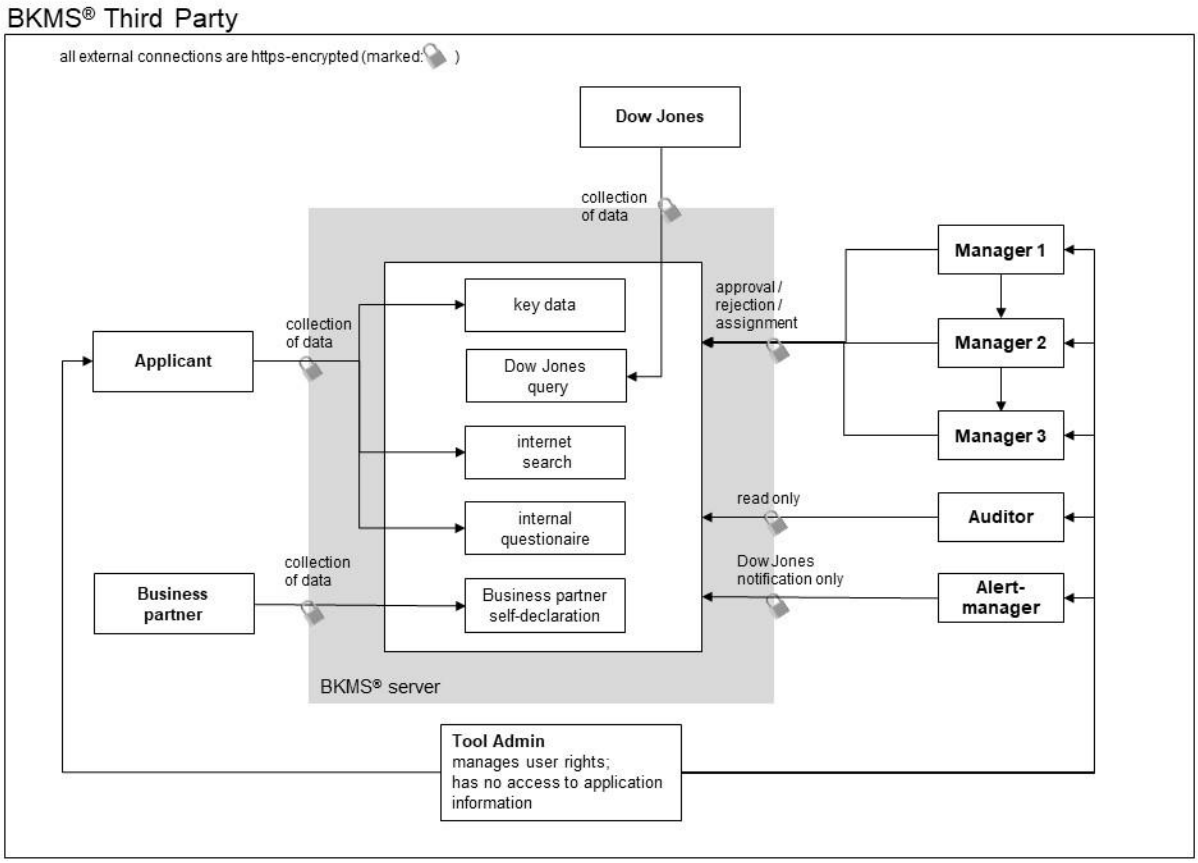

Figure 6: Data flow BKMS® Third Party

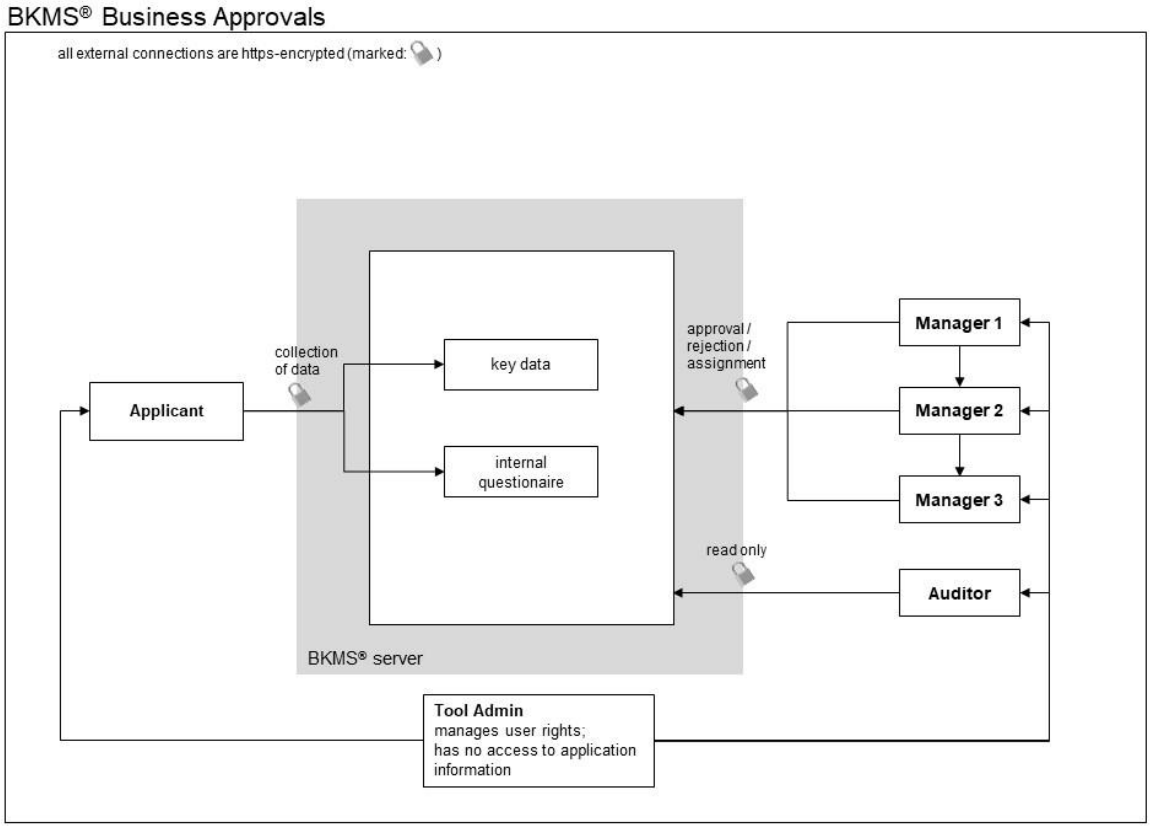

Figure 7: Data flow BKMS® Business Approvals

15. Privacy-enhancing functionalities:

The ToE is designed in a way that only persons explicitly authorized by the customers of Business Keeper AG can access personal data in clear text. By contrast, neither Business Keeper nor the data centers are able to access (unencrypted) personal data. In this regard, the ToE clearly stands out from competitors in the market.

The confidentiality of the personal data is ensured by an authorization concept, which allows the allocation of very differentiated access rights.

Service descriptions and information on data processing are exemplary in terms of transparency and enable the implementation of the rights concerned in an optimal manner.

Organizational and technical measures taken by Business Keeper AG exceed the legal requirements. The Contractor sensitizes the user in an exemplary manner to compliance with data protection, through a privacy statement. The data centers in which the components of BKMS® System are located provide for a high degree of physical security. The data protection and security measures

developed and implemented by Business Keeper AG are also exemplary in light of the privacy-by-design principle.

16. Issues demanding special user attention:

Using BKMS® Third Party, the user should take in mind the following: The options external data source of the Dow Jones Risk & Compliance watch list or search engines via internet are not part of the ToE. If the user chooses to make use of these options, then s/he has to examine the legitimacy of the respective processing thoroughly. In addition, users should keep in mind that it would be critical to use this module for applicant or employee screening or to make automated individual case decisions.

In general, users of the ToE qualify as controllers and are thus responsible for the data protection compliant use of the BKMS® Compliance System.

17. Compensation of weaknesses:

There are no requirements assessed as "barely passing".

18. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Privacy by desing and by default	adequate	The ToE is designed in a way that only allows persons explicitly authorized by the customer to access personal data in clear text. Neither Business Keeper AG nor the commissioned data centres can access (unencrypted) personal data. Furthermore, BKMS® System allows making personal data unrecognizable by using a special "data privacy function".
Transparency	adequate - excellent	Documentation and privacy leaflet are informative, up-to date and understandable. Business Keeper AG also provides a security policy, an account specification document 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 centers located in Germany / Switzerland meet 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 within a certified ISMS 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 data subject requests in the privacy leaflet.

Figure 8: Decision Table

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, 2020-05-04 Alisha Gühr

Place, date	Name of Legal Expert	Signature of Legal Expert

Bremen, 2020-05-04 Dr. Irene Karper

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.

Sebastian Meissner

Digitally signed by Sebastian Meissner
DN: cn=Sebastian Meissner, o=EuroPriSe GmbH, ou=EuroPriSe CA, email=meissner@european-privacy-seal.eu, c=DE
Date: 2020.05.14 09:25:31 +02'00'

Place, Date	Name of Certification Authority	Signature