Short Public Report

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

   EQS Integrity Line, v. 2.0, function as provided in May 2021
   EQS Integrity line is a processor service, provided by the EQS Group AG

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

Company Name:	EQS Group AG
Address:	Karlstraße 47, D-80333 München
Contact Person:	Lorenzo Trevisiol, Senior Compliance Expert EQS
E-Mail:	lorenzo.trevisiol@eqs.com
Phone:	+41 (0)44 515 94 44

3. Time frame of evaluation:

   Evaluation started: 31-08-2020

   Evaluation ended: 05-06-2021.

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

Name of the Legal Expert:	Alisha Gühr
Address of the Legal Expert:	c/o datenschutz cert GmbH, Konsul-Smidt-Str. 88a, D-28217 Bremen
Name of the Technical Expert:	Dr. Irene Karper and Christopher Stradomsky
Address of the Technical Expert:	c/o datenschutz cert GmbH, Konsul-Smidt-Str. 88a, D-28217 Bremen

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):

ToE is the IT-based service EQS Integrity Line of EQS Group AG. The ToE includes 3 packages Basic (BA), Best Practice (BP) and Best in Class (BC), including the standard modules

- "Secure Reporting System"

- "Case Management".

The ToE also includes the optional modules / functions that can be booked by customers as add-ons:

- Translation Module for connecting translation agencies via a specific frontend and via an interface to automated translation services from DeepL (translation agencies and DeepL are not part of the ToE)

- Phone Intake Integrity Message Service (automated caller service)

- Phone Intake EQS Integrity Line to connect call centers via a specific frontend (call centers are not part of the ToE)

- E-mail Intake for messages via a specific e-mail account of the customer

- Ombudsman / Multitake platform to connect ombudsman offices via a specific frontend (ombudsman offices are not part of the ToE)

- In the Basic BA package, customers can also contract the administration roles of their EQS Integrity Line system to EQS Group AG, for example if they do not have the human resources to cover those roles internally. This option is not available with BP and BC, where the admin role is a customer-specific role. When EQS Group AG is contracted with the optional administration within the BA package EQS Group AG acts as a processor for this data processing.

The ToE EQS Integrity Line includes the following components:

- Production system with 3 interfaces (frontend / backend, translation and telephone)

- Database server (Maria DB)

- Apache web server

- Development and test system.

The ToE does not include the deployment environment at the customer's site and customer-specific configurations and components, in particular

- the setup or use of individual reports

- the setup or use of customer specific themes for notes

- data processing of call centers connected to EQS Integrity Line

- data processing in the context of the translation activities of DeepL

- data processing by translation agencies connected to EQS Integrity Line

- data processing by ombudsman offices connected to EQS Integrity Line

- the configuration of a language change function (bias) in Phone Intake by EQS Group AG

- the integration of further tools at the customer's site, e.g. case management tools

Furthermore, the ToE does not include

- Apps for tablets or smartphones

- further service or consulting services of EQS Group AG, in particular not:

- ticket systems used as well as the information portal via Confluence.

- EQS Group's own or brokered call centers or translation services

- services for customer-specific configuration and onboarding.

7. General description of the IT-based service:

EQS Integrity Line is a web-based whistleblowing system. It is used for the submission of secure and anonymous reports on possible irregularities in

companies by whistleblowers and for the central administration of reports by case managers in the company. This also includes communication between whistleblowers and case managers while maintaining the anonymity of the whistleblowers.

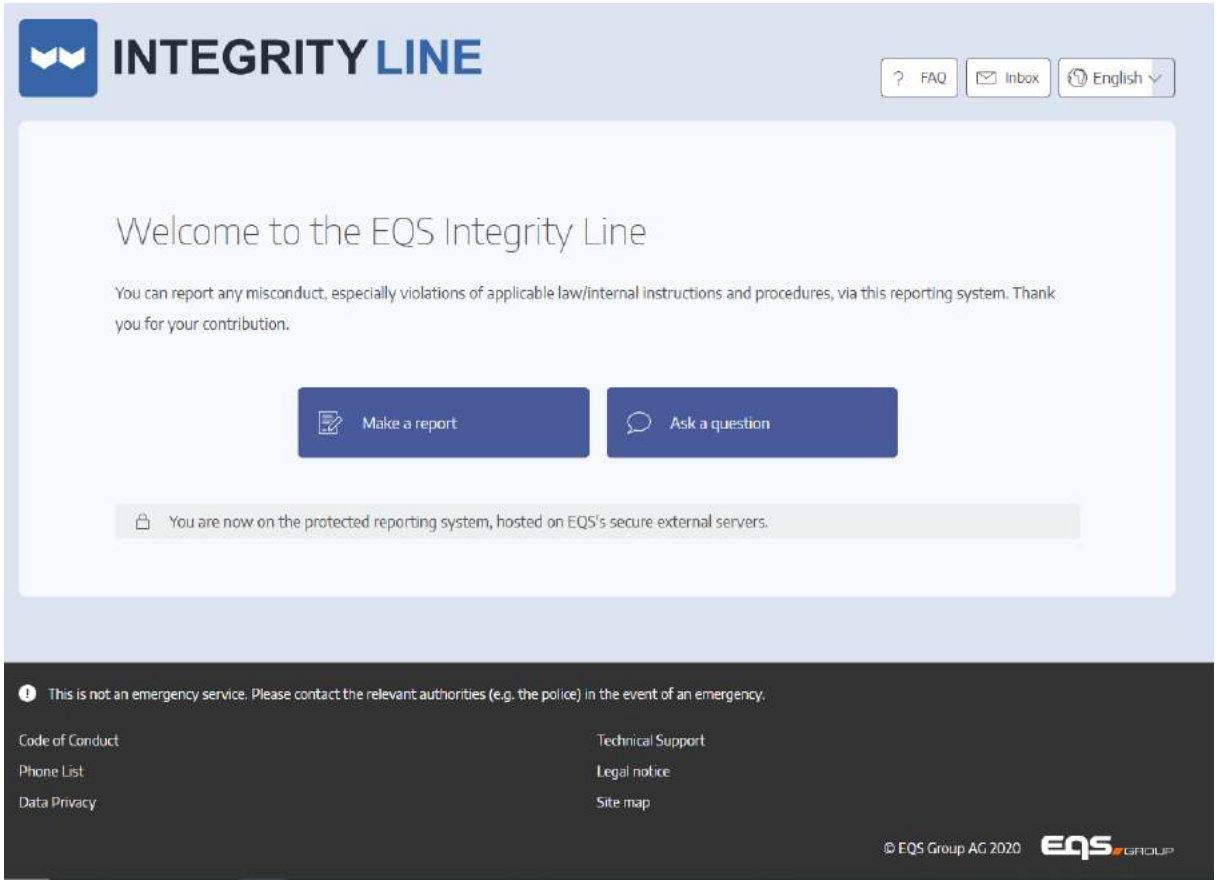


Figure 1 Startpage for whistleblowers

Users are employees of companies, authorities or organizations that use EQS Integrity Line as a whistleblowing system. There are the following roles:

- Whistleblower

- Staff for EQS Integrity Line Backend, which are divided into the roles

- case manager

- user admin

- content admin

- Translators

- Translation Manager

- Callcenter agent

- *Developer*

EQS Integrity Line offers the possibility of translations within the system. It can be used worldwide.

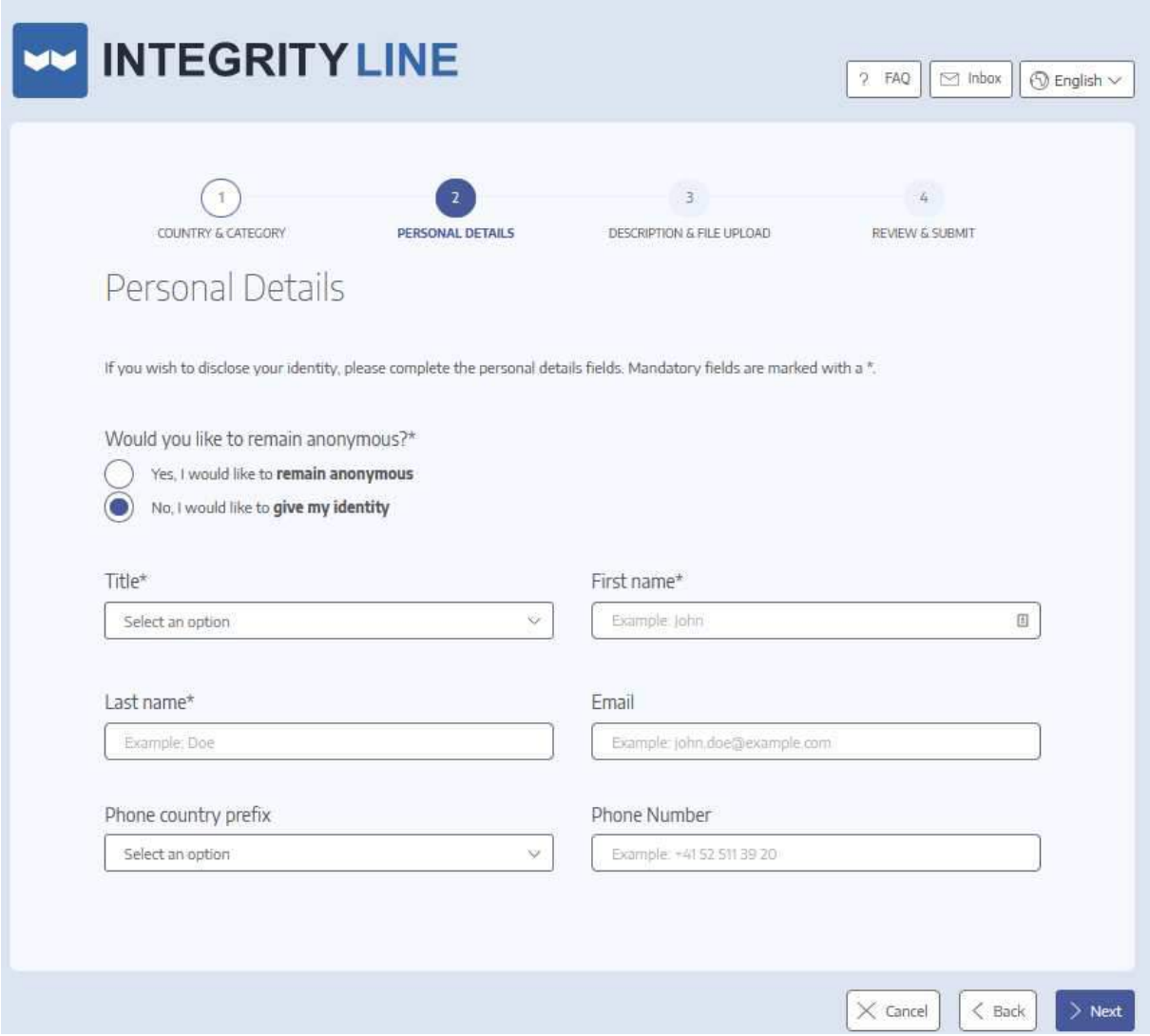


Figure 2 Choice for whistlewblowers to stay anonymous

Personal data is processed. This data includes personal data of the ones who use the system as whistleblowers to submit reports and of the persons whose conduct is reported and in some cases of witnesses to the case. In addition, personal data of employees who are responsible for processing the reports, such as administrators, are processed.

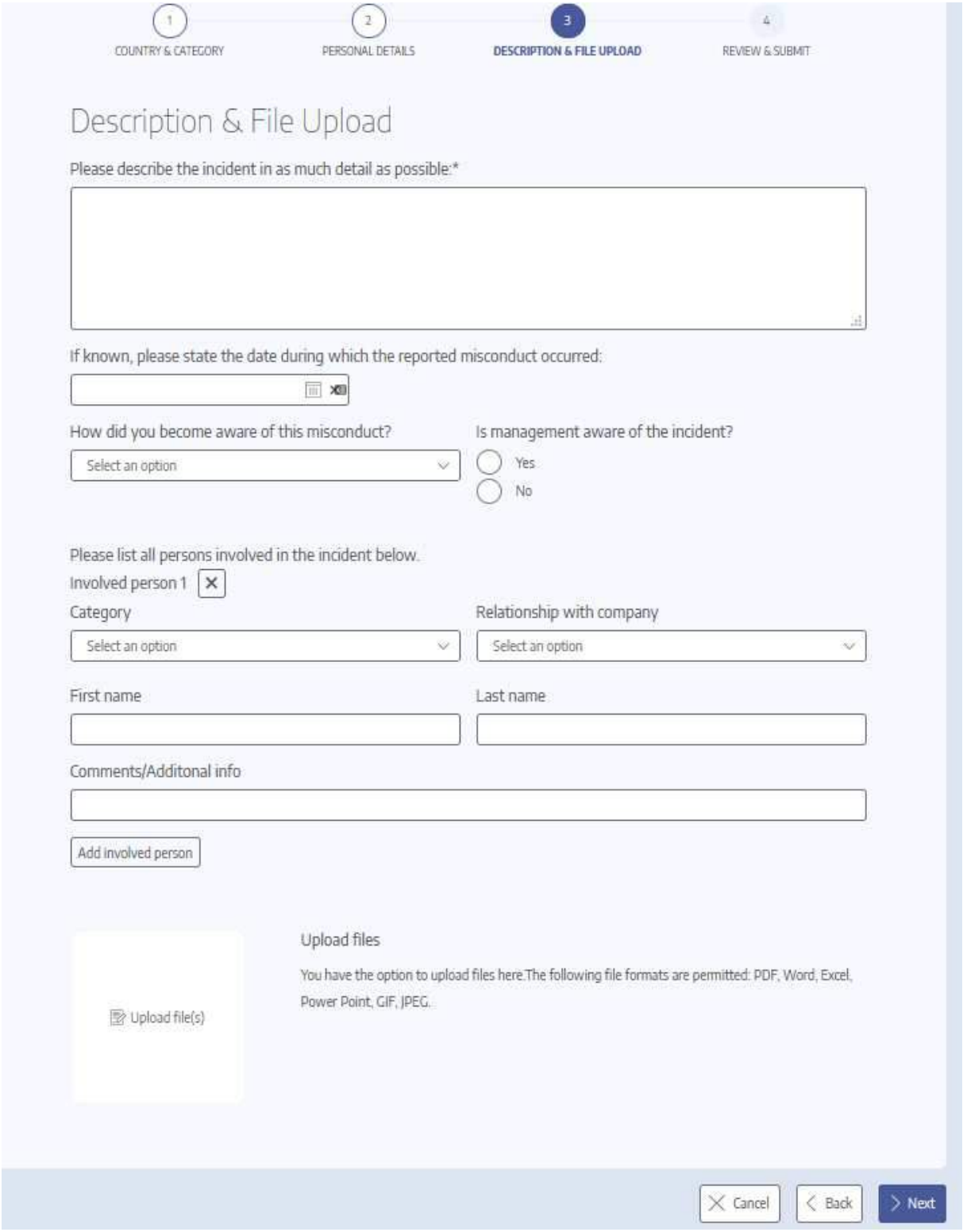


Figure 3 Text fields for case report

EQS Integrity Line is developed and maintained by EQS Group AG as Software as a Service (SaaS) on behalf of the customer and operated in data centers in Germany (Munich) and Switzerland (Winterthur). Customers can choose one of the two data centers. Additionally, backup servers are located in two separate data centers in Basel, Switzerland and in Munich, Germany. Since neither

hardware nor software is provided to customers, but a service of data processing in the web-based system, it qualifies as an IT-based service.

EQS Integrity Line is offered, developed and maintained by EQS on behalf of users via remote maintenance. The programming and implementation of EQS Integrity Line is carried out by EQS employees at the respective customer.

EQS Group AG Germany is supported for the administration of users (customers), implementation and onboarding during the introduction of EQS Integrity Line, as well as for the administration of booked options and modules by

- *EQS Group AG | Hardturmstrasse 11 | 8005 Zurich Switzerland*
- *EQS Group SAS | 3, Rue Tronchet | 75008 Paris France*

both of which act as processors.

Andeo AG provides web application development, hosting and IT support for EQS Group AG within the EQS Integrity Line data centers in Switzerland, while indevis IT-Consulting and Solutions GmbH provides these services for the German data centers.

The processors Indevis GmbH and Andeo AG and all data centers have valid ISO 27001 certifications, which cover their services regarding EQS Integrity Line.

8. Transnational issues:

   Since the EQS Integrity Line is a web-based application it can be used worldwide. Organisations deploy the modules at their branches within the EU, the EEA or worldwide. EQS Group 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 are located, depending on the choice of customers, in high security data centres within the Federal Republic of Germany or in Switzerland.

9. Tools used by the provider of the IT-based service:
   None.
10. Edition of EuroPriSe Criteria and Commentary used for the evaluation:

    Criteria: January 2017 / 'Commentary: May 2017
11. Evaluation methods:

The evaluation included the conduction of a regulatory analysis, use of test accounts, evaluation of product documentation and implementation, respective measures and their efficiency to minimize the risks, evaluation of relevant websites within the ToE and interviews with representatives of the applicant, testing of encryption, website checks by means of browser-based tools (cookies, tracking tools, encryption).

The evaluation of relevant documents included, in particular, security guidelines, password conventions, reports of penetration tests and reports relating to certifications of data centers.

12. Evaluation results:

The following results were found within the framework of the legal and technical evaluation:
EQS Integrity Line is a web based whistleblowing system which is implemented as an individual virtual machine for customers. Whistleblowers reach the system via the frontend while Case Management is accessible via the backend system.

Implementation of legal requirements

Customers of EQS Group AG qualify as the controller of the processing of personal data in relation to the use of EQS Integrity Line. EQS Group AG on the other hand qualifies as processor on behalf of the controller (i.e., their customer). The data centers are located in Germany or in Switzerland and qualify as processors to EQS Group AG ("subprocessor"). For customers who choose Switzerland as their data center location EQS Integrity Line is hosted in a data center of AXA Versicherungen AG in Winterthur, Switzerland (server housing) by Andeo AG in Winterthur. For customers who choose Germany as their data center location EQS Integrity Line is hosted in a data center of noris network AG (server housing) in Nuremberg by indevis IT-Consulting and Solutions GmbH. Other subprocessors include the EQS Companies EQS Group AG (Switzerland) and EQS Group SAS (France) for the administration of customers, implementation and onboarding during the introduction of EQS Integrity Line, as well as for the administration of booked options and modules.

Neither EQS Group AG nor the data centers can access clear text data within the individual EQS Integrity Line of a customer. All data is encrypted. EQS Group AG offers a contract template to customers, which meets the demands of a controller – processor (Customer – EQS Group AG) agreement as required by EU data protection law. The sub-contracts between EQS Group AG and their processors,

namely further EQS sister companies and the data centers meet these legal requirements, too.

EQS Group AG supports their customers by privacy-compliant default settings and an informative and comprehensible leaflet containing information on relevant data protection requirements and best practices.

External bodies, such as ombudsmen, may be embedded in the workflow via specific frontends in EQS Integrity Line. If they may decide about the review of a report to a greater extent these external parties qualify as controller. If access to personal data within EQS Integrity Line is granted to those external parties, this access constitutes a transmission in the meaning of EU data protection law, which requires a legal basis.

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.

From a Data Protection Perspective, 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 reports about violations of "soft factors" such as ethical rules or codes of conduct are not generally permissible. These reports may only be justified exceptionally when not barred by interests or fundamental rights of the data subjects.

Data processing in EQS Integrity Line 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 data subjects must be given the opportunity to object on grounds relating to their particular situations.

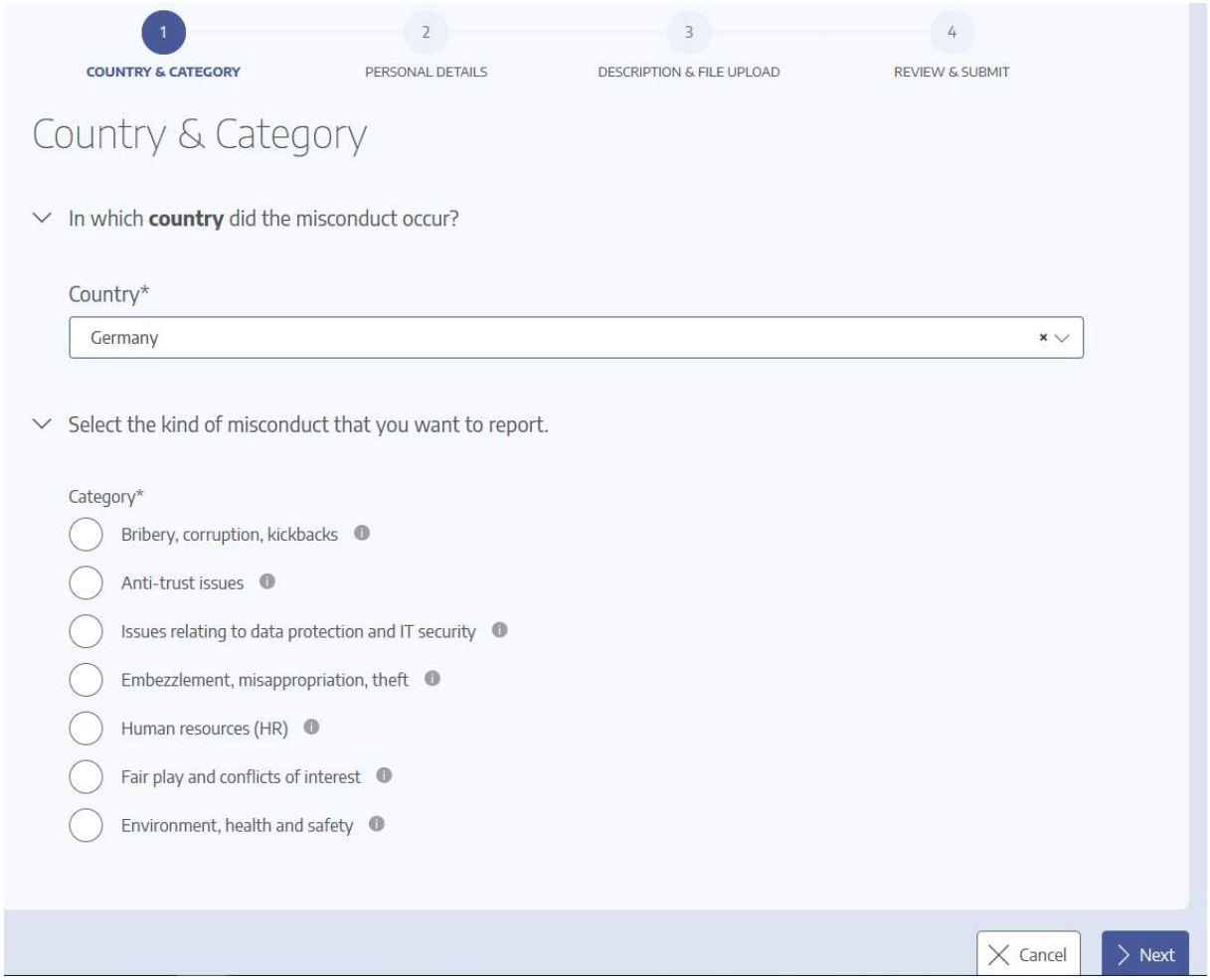


Figure 4 Choice of categories

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, since effective consent cannot be obtained from defendants and witnesses to a case without jeopardizing the means of a whistleblowing system.

In addition, occasionally sector-specific regulations may exist in the individual Member States, e.g. in Germany, Section 25a (1) sentence 6 no. 3 KWG (for

credit institutions) and Section 23 (6) VAG (for insurance companies) should be mentioned. Another example is Art. 8 para. 3 Sapin II in France. Customers of EQS Group AG may rely on the services of external examiners (third parties). In such a case, the disclosure of personal data to these third parties requires 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. On the other hand, a transfer to offices in third countries outside the EU and the EEA 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, 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. Standard contractual clauses have to be backed by additional safeguards, f.e. encryption, in order to provide appropriate level of data protection on an organizational and technical level.

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. In relation to the processing of data of defendants and witnesses to a case effective consent can also not be obtained without jeopardizing the means of a whistleblowing system.

Art. 88 GDPR is relevant for the processing of employee data. This opening clause of the GDPR 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). Works agreements can also be considered as a legal basis (cf. also Recital 155 GDPR).

In most cases the regulations of Art. 10 GDPR will not be applicable when using EQS Integrity Line as a whistleblowing tool, however should they be applicable it is the controllers obligation to bring about official supervision.

In addition, Directive (EU) 2019/1937 on the protection of persons who report infringements of Union law, also known as the EU Whistleblowing Directive, is designed to raise the protection of whistleblowers to a uniform level across the EU and applicable in the context of infringements of Union law. Essential requirements are contained in Art. 17 and Art. 6 of the Directive. According to Art. 17 (2), personal data that are obviously not relevant for the processing of a

specific notification shall not be collected or shall be deleted immediately if they were collected unintentionally. This corresponds to the principle of data minimization, which are met by EQS Integrity Line. The directive also requires companies and organisations with 50 or more employees and municipalities with 10,000 or more inhabitants to setup a professional and GDPR-compliant whistleblowing system. Without prejudice to existing obligations under Union law with respect to anonymous reporting, 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 obliged to receive and follow up anonymous reports of infringements. EU Member States may accordingly provide for other rules regarding the anonymity of whistleblowers. The directive will have to be transposed into national legislation by all Member States until December 2021. To date no country has transposed the directive yet. The interaction of this directive with the data protection requirements of the GDPR and any national regulations will then have to be considered in more detail in following evaluations.

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 set on user terminals when they log into EQS Integrity Line in order to maintain the session. Users are informed about the use of cookies in a document "Quick Onboarding Guide" and a privacy leaflet. 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 deletion, pseudonymisation, anonymization

Case content can be deleted or anonymized, as well as archived by the case manager. Anonymization is applied after the investigation is complete. All packages (BA, BP, BC) in EQS Integrity Line include a GDPR module which offers data protection functionalities, one of which is an anonymization. Content of cases can be anonymized by authorized Case Managers by erasing any personal data refences by searching, deleting and substituting terms. This function can also be used for attachments and free text fields within EQS Integrity

Line. Anonymization is irreversible. Customers can define deadlines to remind users of the obligation to anonymize at specific times.

Archived cases and messages can be reactivated with the appropriate authorization. A dual control principle can be configured for all actions at the customer's request in the BP and BC packages.

If the optional e-mail message channel is integrated, it is possible that the messages in the e-mails are stored on the user's e-mail server, depending on the configuration. Customers are made aware in the privacy leaflet that these must be deleted immediately.

When a user is deleted, all rights are revoked and all user information is deleted, except the username, which cannot be deleted due to the necessity to identify the actions of the user within revision control in the audit trail. Deleted users are only displayed to the User Admin for revision purposes. Final deletion is facilitated when customer systems are deleted and EQS Integrity Line no longer used. The user is informed of this in the privacy leaflet, where EQS Group AG recommends that the User Admin edits the user's data before deletion (surname and first name are replaced by a pseudonym e.g. Case Manager 1).

Activity logs, which contain user name, date, time and action, cannot be modified or deleted by the user, due to tracking of the processing of reports in order to comply with longer audit routines of auditors as well as the long duration of legal proceedings and statutes of limitations. At the customers request, the retention period of the activity logs can be shortened.

In addition, EQS Integrity Line 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.

Security aspects

EQS Group AG has a certified information security management system in accordance with ISO/IEC 27001 for the scope “development and operation of

web-based applications" at the locations in Germany (Karlstrasse) and Zurich (Hardtumstrasse). The data centers in Germany and Switzerland 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.

During onboarding process EQS Group AG has by default two Admin Users to configure the system according to the customer's needs. While these users have access to case data in principle at this point, there is no productive case data on the system yet, so EQS employees do not have unauthorized access to customer data. Only after the onboarding and training period is complete will the platform go live. EQS IT then performs a cleanup and deletes all case data and User Admin accounts of EQS employees. Old accesses and keys of EQS employees are thus rendered useless and no longer grant access. Subsequently, all new data is encrypted exclusively by User Admins as well as Case Managers of the customer according to the defined authorization concepts.

An exception applies when using a multi-client system in the Basic Version. Here EQS manages the "User Admin" account on behalf of the customer, but without case manager rights on case level. Criminal misuse of the admin role by EQS employees to create their own Case Manager users with access rights to cases cannot be ruled out, but the experts believe this risk is low. Not only would it constitute a breach of contract by EQS, any abuse would be irrevocably logged and traceable in the system's user audit trail and case related audit trail, which is anytime visible to the client. EQS employees work according to instructions and are trained as well as committed to confidentiality.

EQS Group AG recommends that all users use the password policy setting of at least "medium", which is set to 8 characters including upper and lower case letters and numbers and must be changed every 90 days. Low includes only 6 characters, but is not recommended. The user is advised of the obligation to use secure password policies in the data protection notice (Appendix 7) Section 8.2 on page 11.

Data subject rights

EQS Group AG provides information on their website and in a privacy leaflet on how to use EQS Integrity Line in compliance with data protection law, especially how to implement processes dealing with data subject rights and how to react on data subject requests.

13. Data flow:

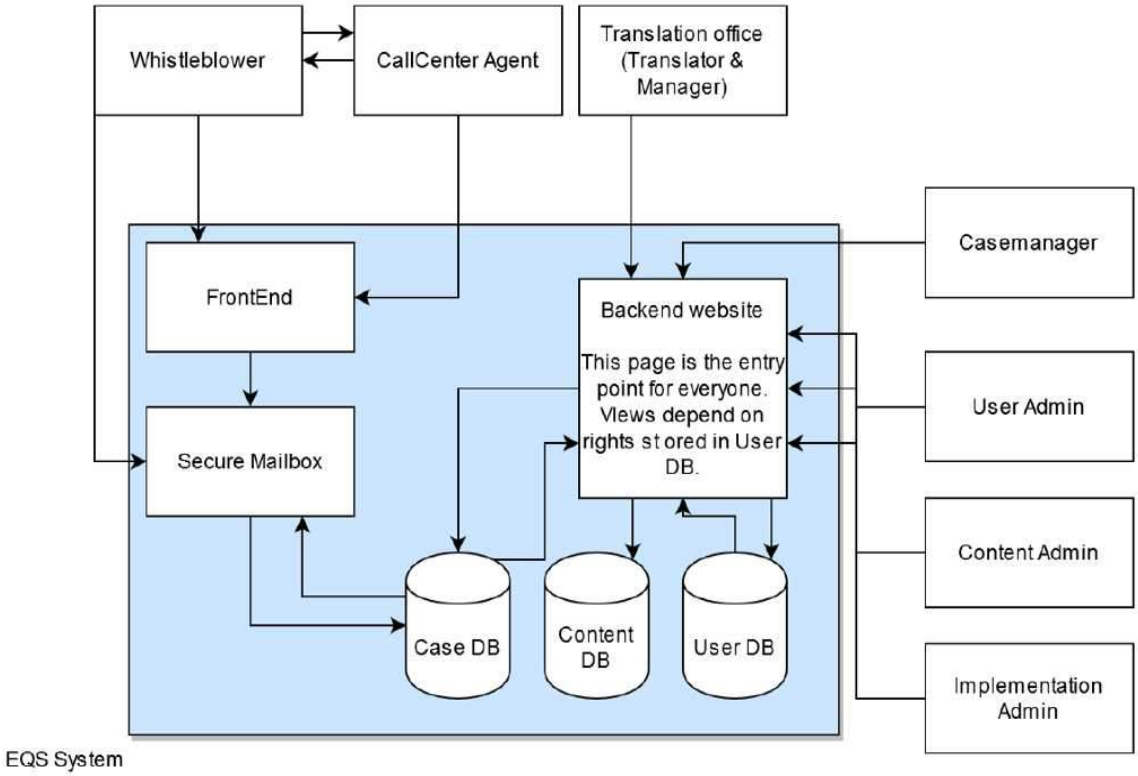


Figure 5 Data flow EQS Integrity Line based on Intake via browser-based frontend

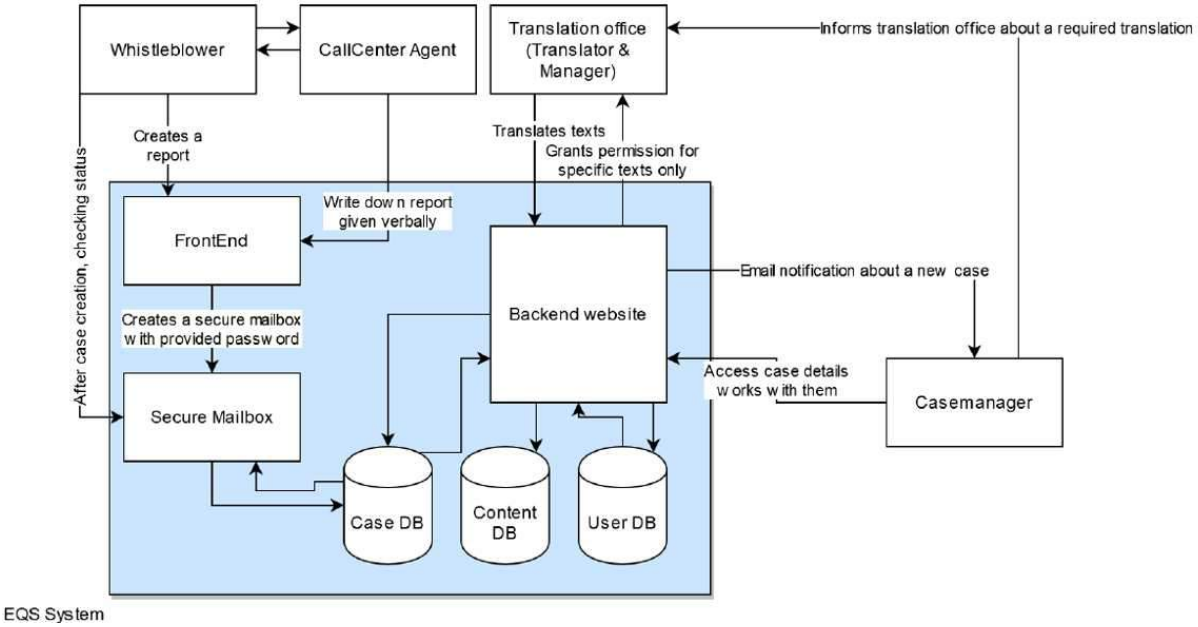


Figure 6data flow EQS Integrity Line with voice intake and translation

14. Privacy-enhancing functionalities:

    - Service descriptions and information on data processing are transparent in an exemplary manner and enable the implementation of data subject rights in an optimal way.

    - Organizational and technical measures taken by the contractor for data security and data protection go beyond the legal requirements:

    - The processor raises user awareness of data privacy compliance by provision of privacy documents like the privacy sheet or privacy document samples.

    - EQS Group AG and the data centers in which the components are located have a high level of physical security and hold ISO/IEC 27001 certifications.

15. Issues demanding special user attention:

    Not applicable.

16. Compensation of weaknesses:

    Not applicable.

17. Decision table on relevant requirements:

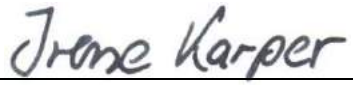
EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*adequate*	*EQS Integrity Line service offers privacy enhancing functionalities like the anonymization module which*

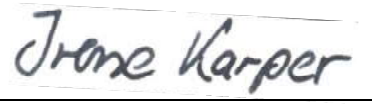
		support the limitation of a data processing to the necessary extent. The user is made aware of the most data minimizing handling of free-text fields in EQS Integrity Line.
Transparency	*adequate*	*EQS Integrity Line documents are informative, up-to date and understandable. In particular, the privacy leaflet provides a clear and concise overview of best practices.*
Technical-Organisational Measures	*adequate*	*EQS has a certified information security management system in accordance with ISO/IEC 27001.The physical location of the servers of EQS Integrity Line in ISO/IEC 27001-certified data centers in Germany or Switzerland support the high level of IT security measures.*
Data Subjects' Rights	*adequate*	Users of *EQS Integrity Line are comprehensively made aware of privacy aspects and best practices. Privacy Tools like the anonymization module and reminders support implementation of the data subjects rights.*

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, 02.06.2021	Alisha Gühr	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Bremen, 02.06.2021	Irene Karper	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Bremen, 02.06.2021	Irene Karper	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Bremen, 02.06.2021	Christopher Stradomsky	
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.

Place, Date	Name of Certification Authority	Signature