Short Public Report

RISER-Service

Recertification No. 4

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

IT-based service:	*Registry Information Service on European Residents („RISER-Service“)*
Functional status:	May 2020.

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

Company Name:	RISER ID Services GmbH
Company Address:	Rudolfstraße 9, 10245 Berlin, Germany
	Web: www.riserid.eu
Contact Person:	Mr. Stefan Göthe

3. Time frame of evaluation: 2020/05-02 – 2020-11-11

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

Name of the Legal Expert:	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):

Components related to the service:

- RISER Internal Client
- RISER Application including eMA monitorings
- RISER Customer-, Supplier- and Registration-Authorities-Portal

Not part of the ToE are:

- The use of RISER via smartphone or tablet
- - the user's operating environment
- - the hardware components and the operating system used in the data center
- The inclusion of relocation databases
- -The service regarding the enrichment of birth data (by Schufa Holding AG)
- Supplier credit agencies of the suppliers (broker) and population registers
- further services of RISER ID Service GmbH.

7. General description of the IT-based service:

RISER ("registry information service on European residents") is an IT-based service. RISER is offered by the RISER ID Services GmbH as registration data broker to obtaining registration information on behalf of public or private bodies. These can be simple and to a limited extent also advanced official register inquiries for Germany, Switzerland and Austria via RISER.

Customer-Inquiries for different countries or communities are submitted via a central web portal at https://www.riserid.eu. RISER distributes a request to the respective register office. The register office processed the request and sends the result back to RISER.

Following this, the result can be downloaded from the web portal by the customer. The results are deleted, taking into account the contractual retention period.

When obtaining register inquiries, the RISER ID Services GmbH prepares the request and result data, by checking manually the incoming or outgoing data for plausibility, adapted format structures and inconsistent results.

Figure 1 Workflow – simplified view

Users of RISER are companies and public bodies, which are based in the EU, suppliers (broker services) and registration authorities. Users can log in with name, ID and password on the closed user-group and maintain person related master data for their account, obtain performance records, or process information.

The customer can request this information through single inquiries or through mass inquiries. For a single inquiry, data is directly entered into a form, which is adapted to the requirements of the relevant national or local registry office. Mass inquiries are catered for by transferring a file containing multiple data sets with inquiries. The customer receives a collection of orders, indication of price, and the request to confirm the selection with "OK" which places the order into the user's account. RISER processes the confirmed request and provides the registration results in the account again.

With the optional "eMA-Monitoring" an additional service is offered to improve the quality of services. The customer will be informed by RISER in case of time-delayed updates in the population register. The customer is informed when selecting this additional service, if the registration authority gains new information, and can selectively stimulate a new

request to this person. In the course of eMA-Monitoring neither personal request and result data is stored permanently for own purposes, nor is the data released to third parties (so-called addresspooling). eMA-Monitoring is subject to evaluation.

Addresses can optionally be determined by RISER in the database of the Deutsche Post Adress GmbH & Co. KG and new: ABIS GmbH. In addition, RISER provides the optional potentiality to determine dates of birth to a requested person at the Schufa Holding AG, if there is a legitimate interest. Moving database and credit agency are not subject of the evaluation.

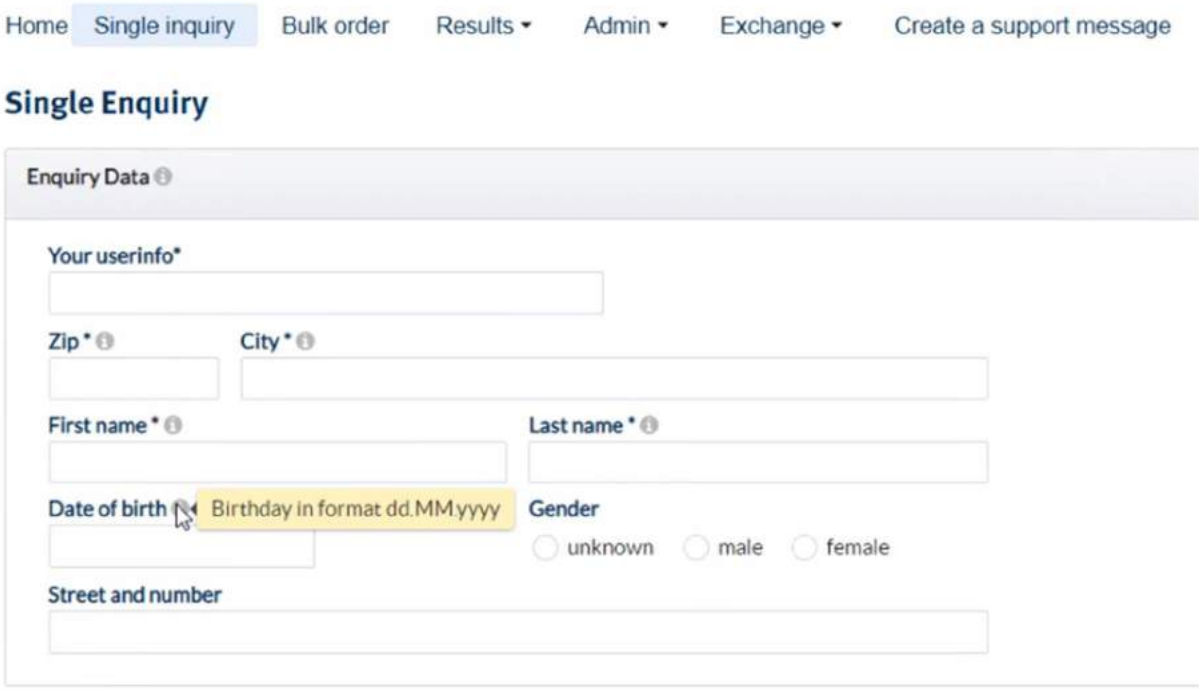

Figure 2 example for an inquiry

In the standard design of RISER inquiry and results data for customers are stored on an archiving server for six weeks. Customers can set a shorter retention period. Thereafter the data is adopted by the revision database of RISER, which serves the verification and accounting for reporting to authorities and customers. The inquiry and results data are kept 90 days before made anonymous and the receipt archived with no personal connection.

Order and result data will be made available to the customer for download after being transmitted by the registration office for 42 days in the customer portal. Then the order and result data are transferred to the revision database.

The RISER ID Services GmbH undertakes the register query process as well as the preparation of the result data on behalf of the customer at the site in Berlin. The RISER IT systems are housed on behalf of RISER ID Services GmbH in the datacenter of

q.beyond AG, (former QSC AG) in Munich. This is a pure housing. The IXSYS EDV Systemberatung in Munich is commissioned to undertake the operation of IT-systems through the RISER ID Services GmbH. For the implementation of conventional (usually written) registration inquiries the RISER ID Services GmbH makes use of sub-contractors based in Germany, Swiss and Austria.

8. Transnational issues:

The RISER service is provided for the countries Germany, Austria and Switzerland.

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

None.

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria Catalogue, January 2017.

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

A number of processes have been put in place to improve the quality of the data and to minimize requests for data and information to the essential. Futhermore, the internal client (monitoring systems) were updated.

12. Changes in the legal and/or technical situation

RISER GmbH moved to other premises in September 2020. The operative business of the RISER service now takes place in the offices of RISER ID Services GmbH in Rudolfstraße 9 in 10245 Berlin. The technical and organizational data protection for the new location have been adapted by RISER, changed in the processing agreement and evaluated in this recertification.

RISER has to implement the requirements of the reporting legislation, which have frequently changed during the previous certification period. These requirements are implemented in the corresponding forms as well as in correspondingly changed contractual bases with the users and have been continuously evaluated since the last re-certifications. Due to the amendments to § 49 BMG as of 01.05.2017, in order to identify the data subject in the registration register, inquirers in RISER must enter two additional search characteristics of the data subject in addition to first name and surname. RISER has defined the address as "two" search criteria. Furthermore, the search characteristic

"gender" was allowed again, although a search together with the characteristic marital status was excluded.

Since the last evaluation new processors have been introduced.

Finally, ABIS is commissioned to provide Post Adress Move or the relocation database, but only if a RISER customer separately commissions this. Like Deutsche Post Adress, ABIS belongs to the same group of companies DPA as RISER. However, the relocation database is not part of the ToE. Therefore, this service provider is not relevant for the ToE.

Schindler Technik AG provides IT service support for the IT in the offices of RISER in Berlin. The order processing mainly concerns employee data of the RISER company and is therefore only indirectly attributable to the ToE from the evaluators' point of view.

Rhenus Data Office is commissioned with the destruction in accordance with DIN 66399 and destroys data carriers used in the internal administration of the RISER company. The order processing also mainly concerns employee data of the RISER company and is therefore only indirectly attributable to the ToE from the evaluators' point of view.

RISER has concluded processing agreements with all mentioned service providers in accordance with Art. 28 DSGVO or that the customers conclude their own contract for order processing with ABIS according to the RISER model. The change of the service providers is displayed to all customers accordingly, e.g. in the appendix to the processor agreement. Overall, this is not objectionable.

RISER ID Services GmbH now uses Matomo as a tracking tool for measurement. A consent option via a cookie banner is implemented, in order to inform the user about the use of the related cookies and get consent for the tracking.

A new framework model has been introduced and is intended to replace RISER's previous processor agreement by the end of 2020. The model contract has been evaluated and fulfils the requirements of Art. 28 GDPR.

Each 1.5. and 1.11. of a year a new xMeld standard is introduced. The interfaces to suppliers of RISER will be adapted to the changed standards. At the time of evaluation XMeld version 2.4.2. is implemented in RISER.

The web client was reprogrammed. Process description and user manual were revised.

Information about the ordering party of an inquiry must be given in a clear, understandable and identifiable manner for reporting authorities (e.g. the indication "RA Müller" is not clearly identifiable). RISER therefore now issues error messages to the sponsor for queries which have features which cannot be identified, so that the sponsor can correct the request. This also serves to correct the data set and at the same time implements the requirements of the BMG in this respect, which is not objectionable.

For better monitoring purposes of RISER a dashboard has been implemented. It displays various parameters (e.g. incoming orders, online requests), which give an indication of the "health status" of the system. In this context, additional markers were installed in the system, which generate a message when certain events occur (e.g. water level markers for disk space). Important system processes are displayed in exposed colors. The evaluators assess this monitoring of the RISER systems and their preparation via a "dashboard" as optimization measures for availability and for regular evaluation.

13. Evaluation results:

Using RISER companies and public authorities in Germany, Austria and Switzerland obtain a user-friendly way to assign a registration data broker obtaining registration information. The RISER GmbH is working as a data processor. Rights and obligations are governed by a contract to order data processing, which complies with all aspects of data protection as stated in the GDPR. Also incorporated subcontractors of the RISER ID Services are legally bound by contract and checked regularly.

The scope of the data processing using RISER is tailored to the data required by the respective registration authorities. The auditors verified that RISER serves the purpose to process as few data as necessary and at the same time only relevant data. RISER is constantly being optimized for this purpose.

As far as additional data is entered at all in a request entry in form fields, this is optionally done by the customer. Moreover, RISER doesn’t store data permanently for their own purposes, but reduced the storage time of the inquiry and results data in the standard version to 6 weeks, to allow the customer the retrieval. Then the data is transferred to the revision database of RISER, which serves the verification and accounting to reporting authorities and customers. The inquiry and results data are kept here 90 days before being made anonymous and the billing information archived without any personal reference. Order and result data will be made available to the customer for download after being transmitted by the registration office for 42 days in the customer portal. Then the order and result data are transferred to the revision database.

Also, with the optional eMA-monitoring only dedicated data is used. RISER reduces data to a hash value that cannot be decrypted on the part of the RISER ID Services GmbH. This prevents reuse of results data from the registration authority.

The use of RISER is intuitive. Customers can see at any time the processing steps and what data are in the workflow.

All essential documentation is available in German and English. The information is easily accessible, meaningful and informs the user comprehensively about RISER, the use and the data processing operations.

Registration requests and the use of the provided data must be carried out only on the basis of the registration laws. RISER supports compliance with the respective legal bases by configuring form fields and data records, so that they meet the requirements of the respective registration authority and at the same time are accepted for a request of register information by these.

The data processing using RISER is usually not initiated by the data subject itself but by the customer as the controller. Therefore, the data processing using RISER depends on the interests of all those involved in addition to the legal and contractual bases. The customer is obliged to ensure the compliance with the requirements under the contractual agreement. On the other hand, the registration authority is responsible for the provision of register information on the basis of legislation.

RISER complies with legal requirements for giving a reason and purpose of the information by having the commercial purpose to be specified mandatorily for simple register information of private legal persons from German authorities (§ 44, paragraph 1, sentence 2 BMG). For advanced register information, a legitimate interest in accordance with § 45 BMG must credibly be shown, which is captured by RISER on corresponding data fields and only then passed on to the registration authorities. Also, customers must assure contractually that the requests for register information are not for the purposes of advertising and address trading. They undertake to give a unique business reference in the requests and will be pointed out, as far as possible to specify the date of birth to the requested person in the request to the register information.

In Austria, information from the register of residents is possible on the basis of the Federal Law on Police Registration (MeldeG) and the Regulation implementing the Registration Law (MeldeV). RISER implements the requirements of §§ 16 and 18 MeldeG for information.

In Switzerland, information is obtained from the population register on the basis of cantonal and municipal laws. In the Canton of Zurich, Section 18 of the Law on Registration and Residents' Register (MERG) and Section 16a of the Law on Information and Data Protection (IDG) apply. In the Canton of Berne, Art. 11 of the Cantonal Data Protection Act (KDSG) applies.

In case of legal barriers according to the respective registration law, registration information is not given by the respective authority.

The data minimization in the sense of article 5 GDPR is respected because the user is given the ability to reduce the amount of data to a minimum using RISER.

This applies also for the upstream methods to query a date of birth at the Schufa Holding AG. Pursuant to § 49 para 4 BMG information may only be given, if the applicant has described the requested person with family name or former name and at least one given name as well as with two more data stored on the basis of § 3 para 1 BMG, except the Nr. 1 to 4, 7, 10 and 11, and the requested identity has been proven by the automated alignment of the given data in the request and the stored data. A phonetic search is permissible for surname, previous names and given name. Then the use of the sex of the queried person for a request is now allowed. Furthermore, the date of birth (section 3 para 1 No. 6 BMG) represents the key attribute of the request for the customer of RISER. Since not every customer has the date of birth to the requested person, RISER allows an upstream request to the date of birth at the Schufa Holding AG. Knowing the date of birth, the register information can then be obtained for this person according to § 49 BMG. However, this function is not part of the ToE.

This also applies to the address research in the moving database of Deutsche Post Adress GmbH & Co. KG / ABIS GmbH. This can be done optionally in advance of register information, to update the address. The data subject has granted a consent to the entry into the moving database with a forwarding request. Without having issued a forwarding request or when having revoked the consent, his data is not in the database.

Optional eMA-Monitoring is also proportionate. It serves only quality improvement using hash values. No reuse of registration data takes place but intervenes only in cases where the result data set of the population register is not usable and the possibility of a correction is in the legitimate interests of the customer.

RISER as the controller supports the implementation of the rights of the data subject, by giving the user all the necessary information on the data processing, which would be

required for a notification of data subjects. RISER ID services has also established a well-structured data protection management, which can help the customer if necessary.

The technical and organizational data protection measures taken by RISER are adequate. The certification of the datacenter of q.beyond AG in accordance with ISO/IEC 27001 for the scope "Cloud Services, IT Outsourcing, Housing, Hosting, IT Consulting, Internet, Telephony and Networking" proves their implementation and effectiveness. Technical and organizational data protection and data security measures are contractually binding set with all subcontractors. In this respect the IXSYS EDV Systemberatung participates in the security measures taken on the part of the data center.

RISER portal users are prompted in different places to submit a secure password. The Web pages are encrypted via https and adequately protected against unauthorized reading of communications during data transfer. Matomo is used for webtracking. A consent option via a cookie banner is implemented, in order to inform the user about the use of the related cookies and get consent for the tracking. The cookies used for the statistics via Matomo are, therefore, set with the consent of the website visitor in accordance with Art. 6 Para. 1 lit. a DSGVO. This implements the requirements of the BGH judgement of 28.05.2020 and is not objectionable. It should be emphasized that Matomo is not used on the login pages of RISER and in the user account itself, which was confirmed by the experts.

All system activities in the editing process are logged and processed in the RISER internal client for monitoring and control. The log-data is stored for troubleshooting as well as for abuse prevention for 6 months and then automatically deleted. This is necessary, especially in the case of potential abuse (such as e.g. the use of the account by unauthorized users or for private purposes), because cases are usually detected and claimed by the customer with a considerable time lag in the wake of the accounting control. An evaluation is carried out in case of need, which is plausible. Data encryption is based on a well-structured crypto-concept which is implemented with reasonably safe encryption mechanisms.

Operative business of the RISER service takes place in the offices of RISER ID Services GmbH in Berlin in accordance with an IT-concept. The RISER ID Services GmbH has a detailed and well-structured fault and emergency management as well as a test and approval procedure established and documented.

14. Data flow:

The following figures describe the data flows:

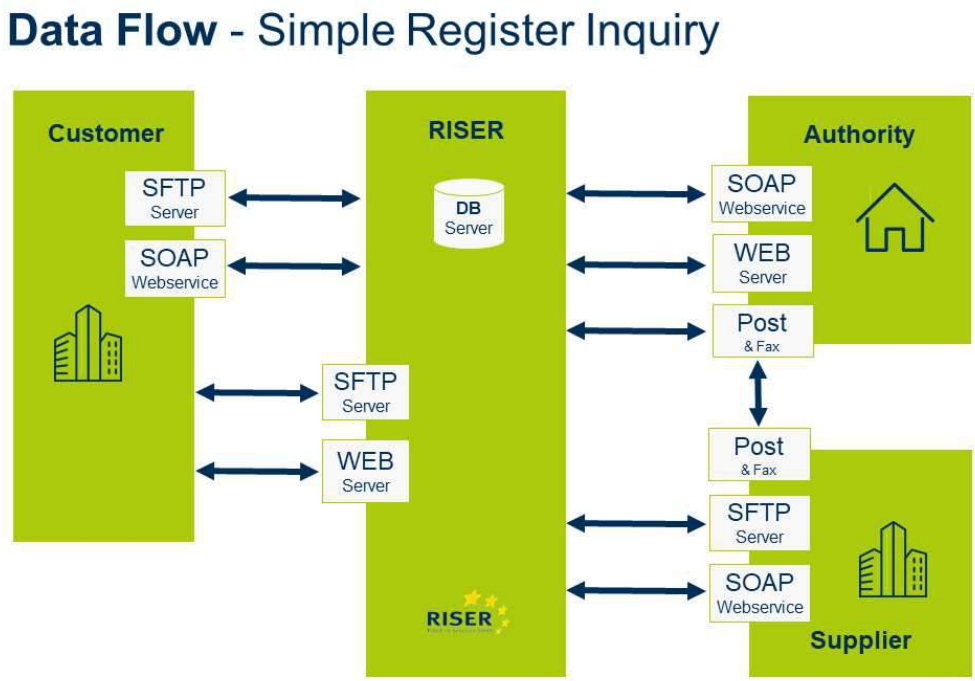

Figure 3 Data Flow – simple register information

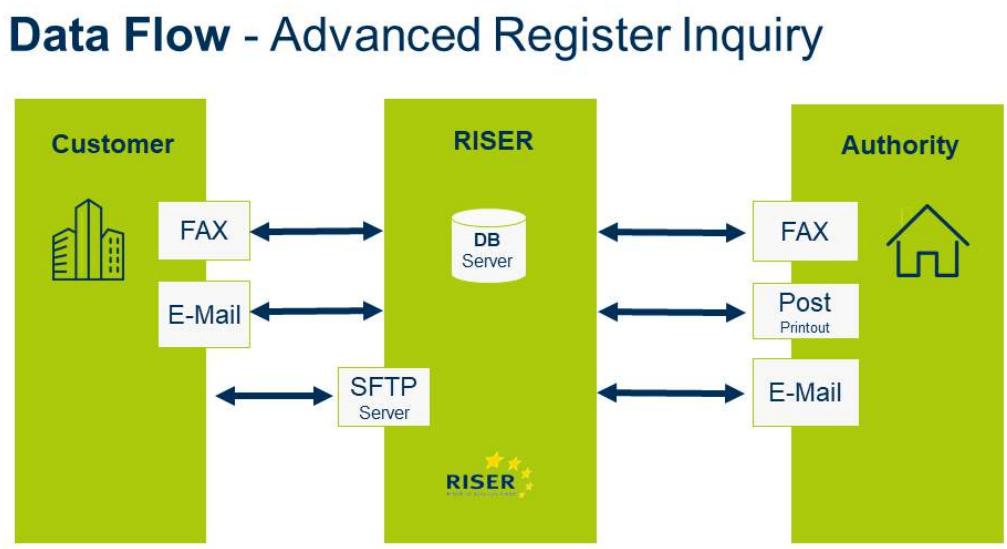

Figure 4 Data Flow – advanced register information

15. Privacy enhancing functionalities:

The scope of the data processing using RISER is tailored to the data required by the respective registration authorities. It can be stated that RISER serves the purpose in terms of data minimization and data avoidance, to process as few data as necessary and at the same time only relevant data. RISER is constantly optimized for this purpose. The current, informative and user-friendly information to RISER enables the user exemplarily, to protect rights of persons affected.

16. Issues demanding special user attention:

None.

17. Compensation of weaknesses:

There is no need for compensation since there is no weakness.

18. Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	adequate	The scope of the data processing using RISER is tailored to the data required by the respective registration authorities. It could be stated that RISER serves the purpose to process as few data as necessary and at the same time only relevant data. RISER is constantly optimized for this purpose.
Transparency	adequate	Documentation and data protection statement are informative, up-to-date and easy to understand.
Technical-Organisational Measures	adequate	Physical access protection, logging mechanisms, backup and recovery mechanisms, incident management and tests and release procedure follow a well-structured approach and are up-to-date and appropriately implemented.
Data Subjects' Rights	adequate	Transparent and up-to-date documentation on data protection and IT security enables users adequately to fulfil the rights of data subjects.

Experts' Statement

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

Bremen, 2020-11-11 Alisha Gühr

Place, date	Name of Legal Expert	Signature of Legal Expert

Bremen, 2020-11-11 Dr. Irene Karper

Place, date	Name of Technical Expert	Signature of Technical Expert

Recertification Result

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

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

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