EuroPriSe
European
Privacy Seal

European Privacy Seal

– privacy at its best

RISER-Service
Short Report

Version History

Version	Date	Reason for Changes	Author(s)
1.0	28-11-2023	Initial version	Arghya Biswas
1.1	05-12-2023	Changes by review team	Sebastian Meissner
1.2	15-12-2023	Editorial changes based on feedback from RISER ID Services GmbH	Arghya Biswas

Table of Contents

List of Figures

1. Type of Certification and Applicable EuroPriSe Specification Documents

Type of Certification

Processing operations by a processor.
Initial certification

Applicable Criteria Catalogue

EuroPriSe criteria catalogue for processing operations by processors (DE) v3.0

Applicable Rules of Procedure

EuroPriSe rules of procedure for processing operations by processors v2.1

Applicable Evaluation Compendium

EuroPriSe compendium of evaluation methodology for processing operations by processors v2.1

Applicable Matrix of Evaluation Methods

Matrix of evaluation types and methods v2.1

2. Name of the Certification Customer and General Information about Them

Name of the Certification Customer

RISER ID Services GmbH

Address of the Certification Customer

Rudolfstr. 9
10245 Berlin
Germany

Membership of a Group of Companies

Yes. Deutsche Post Adress GmbH & Co. KG

Sector in Which Certification Customer Primarily Operates

Public Sector and Business Customers

3. Information on the Target of Evaluation ("ToE Description")

Name of the ToE

RISER-Service

Description of the ToE in Plain Text

RISER-Service (Registry Information Service on European Residents) is a service offered by RISER ID Services GmbH (in the following: RISER ID) for obtaining information from the civil register on behalf of public or private bodies. They can use the Customer Portal at https://kunde.riserid.eu/login.xthml to request information from the civil register for Germany, Switzerland and Austria.

Requests via RISER-Service are forwarded by RISER ID to the responsible registration authorities and are processed by them. As a rule, the information from the civil register is provided electronically. Where this is not (yet) possible, enquiries are made conventionally (by letter or fax).

Via RISER-Service, the result data obtained from the inquiries are then made available to the inquirer (RISER customer) for collection and deleted again, taking into account the contractually agreed period of time. When obtaining information from the civil register, RISER ID processes the request data and the result data via RISER-Service by checking the incoming and outgoing data for plausibility, adjusting format structures, and manually checking inconsistent result data if necessary.

An overview of the RISER-service is depicted below:

Fig 1: Overview of the RISER Service

(Future) Customers first need to submit the following data to be registered on the RISER Customer Portal:

- First and Second name
- Company or Institution name
- Email address
- Telephone Number (optional)

After the processing of these data by RISER ID's sales department, the customer receives the "Agreement on the Use of the European Registration Information Service RISER". Once the contract is concluded, the customer receives login credentials (customer name, user name and a password). Therefore, a link (valid for next 24 hours) is sent to the customer's email address. Customer uses the link to login and assign themselves a new password. The first user can also create new users or deactivate existing users.

Registered users can submit orders for official population registry inquiries.

The login page of the Customer Portal is as follows:

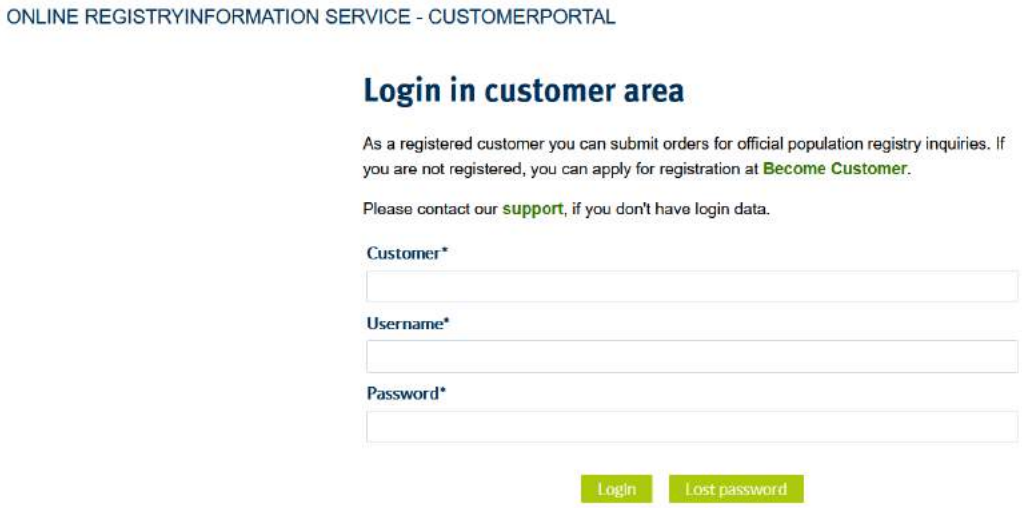

Fig 2: Login page of Customer Portal

After successfully logging in, users can submit an individual enquiry, as depicted in the following illustration:

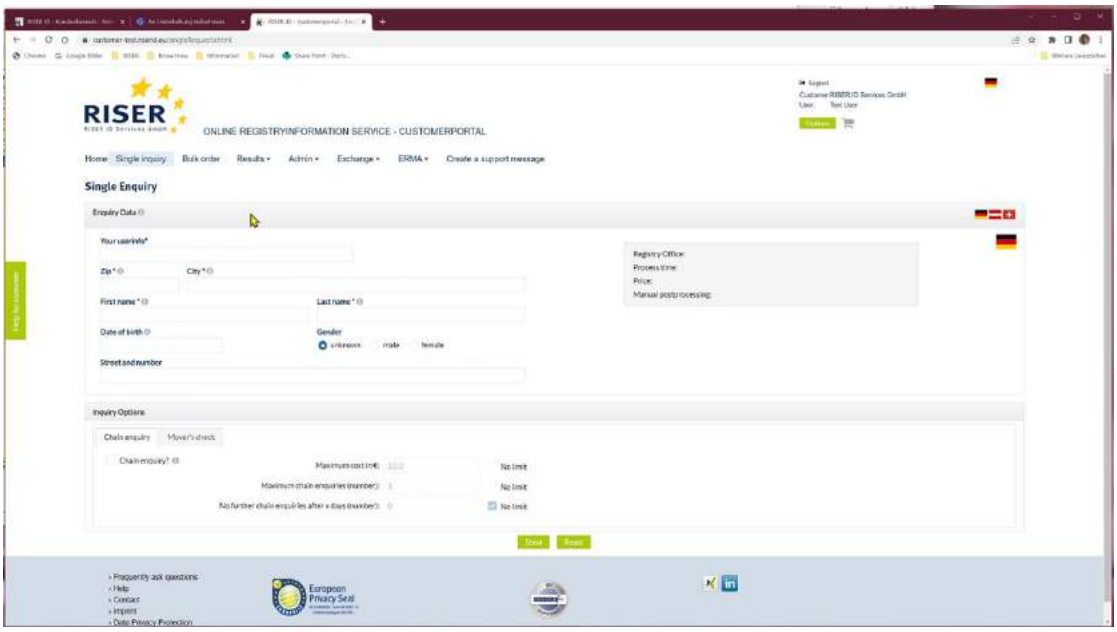

Fig 3: RISER Customer Portal: Single Inquiry

Along with the individual inquiries, customer can also request bulk orders by uploading a list of orders in excel form.

In the account, customer receives a listing of their desired orders, the price information and the request to confirm, and thus to place the order. RISER ID processes the confirmed request and makes the reporting results available in the account. Order overview of a customer is depicted below:

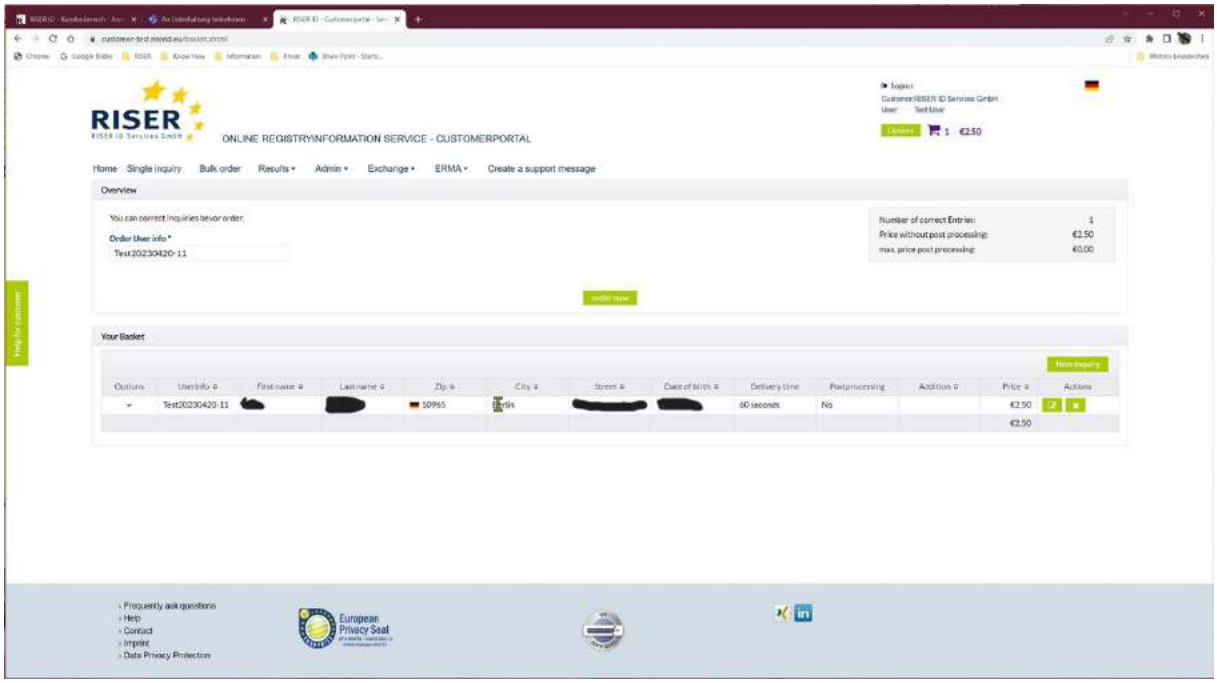

Fig 4: Order Overview

The customer can also view the current status of placed orders in the Customer Portal at any time, as shown below:

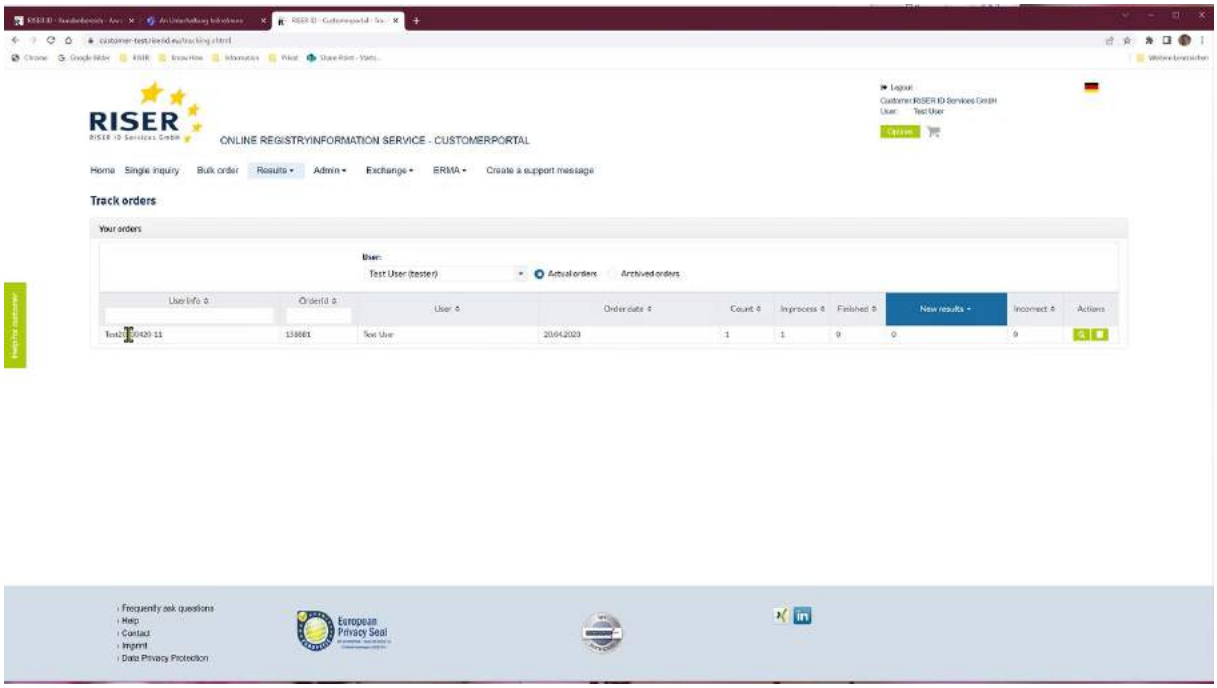

Fig 5: Order Status

The workflow of the RISER Service consists of the following steps

- A customer places an order to obtain information from the civil register. The RISER-Service checks the received request for completeness and determines the registration office responsible for it.
- The request is converted into the respective valid request format and sent to the registration office.
- The registration office performs the search in the civil register and transmits the result to RISER-Service.
- RISER ID receives the result, checks it and makes it available to the customer for collection in the 'Results' section.
- The Client picks up the result.

Specification of Essential Aspects of the ToE

Processing Operations, Processes & Functionalities

The following processes and functionalities are part of the ToE:

- User Registration

- Basic Functions of RISER-Service
  - Processing of the inquiry data and the results
  - Authentication of users when logging in
  - Log file processing

Purpose(s)

- The RISER-Service provides full access to registration authorities in Germany, civil registers in Switzerland and the central civil register in Austria. RISER ID customers use the service to obtain information from these civil registers.
- Enquiries and results are transmitted between clients and RISER ID by electronic means. Where RISER-Service does not have an electronic connection, enquiries are processed conventionally (letter, fax). This is mainly done by subcontractors.

Categories of Data Subjects

The ToE concerns the following categories of data subjects:

- Persons who are registered in the civil register (residents) and about whom information is provided via RISER-Service;
- Customers and their employees who use the RISER-Service application;
- Employees of RISER ID who are handling the requests.

Categories of Personal Data

The following categories of personal data are collected:

- Inquiry and Result data
- User registration and authentication data
- Log data

The following data about the people concerned (residents) are processed in connection with enquiries / results:

- First name
- Surname
- Gender
- Date of birth
- Postcode
- City
- Street
- House number
- Country code (AT, CH, DE)

RISER Service does not process any special categories of personal data.

Relevant Locations

There are multiple locations that are relevant for this ToE:

- The support of the operational business and further development of the RISER-Service and the Internal Client (software for RISER employee use only) take place in the office of RISER ID in Berlin. The IT infrastructure as well as office applications in Berlin Office are managed by Deutsche Post Adress GmbH & Co. KG based in Germany as part of the division of tasks within the group of companies.
- RISER ID's IT systems are located in the data centre of North C Group (formerly known as IP Exchange GmbH) in Germany. This is a pure housing.
- The managed operations of RISER ID's IT systems are provided by Ixsys EDV Systemberatung, Germany.

Transfers to 3rd Countries

The service is also used by customers based in third countries. Specifically, these are (only) customers from Switzerland and the UK.

If enquiries are made to registration authorities in Switzerland, RISER ID transfers the enquiry data to the respective authorities. In this case, RISER ID also uses a sub-processor based in Switzerland.

Consequently, when using RISER service, data may be transferred to Switzerland and the United Kingdom.

For both countries, there are adequacy decisions by the European Commission (Switzerland: 2000/518/EC; UK: (EU) 2021/1772) on which these third-country transfers can be based.

Area of Application

Business Customers, Public Sector

Meaningful Graphical Illustration of the Data Flow

Please cf. figure 6 below.

Processing Operations Forming Part of the ToE

ToE is the RISER-Service, which consists the following components:

- RISER Internal Client (software for RISER employee use only)
- RISER Customer Portal

- Supplier and Registration Authorities Portals (only covered by the ToE with regard to the processing of query and result data)
- User registration and authentication
- Logging

Processing operations not part of the ToE

This section contains a tabular list of all processing operations / components that are closely related to the ToE, but do not form part of the ToE.

In particular, functionalities that are not basic functions of the RISER service, but are only provided on special request of the customer (optional functions), have been excluded from the ToE.

The ToE does not include:

- The Use of RISER Service via smartphones and tablets;
- The operating environment at the user's premises (RISER ID customers);
- The inclusion of relocation database (optional function);
- The service regarding the enrichment of birth data (by Schufa Holding AG) (optional function);
- The processing of mail returns (ReAdress) (optional function);
- Employer identification and address research (optional function);
- Further services provided by RISER ID;
- Email encryption gateway, as there is no exchange of personal data that are relevant to the ToE.

Meaningful Graphical Illustration of the data flow:

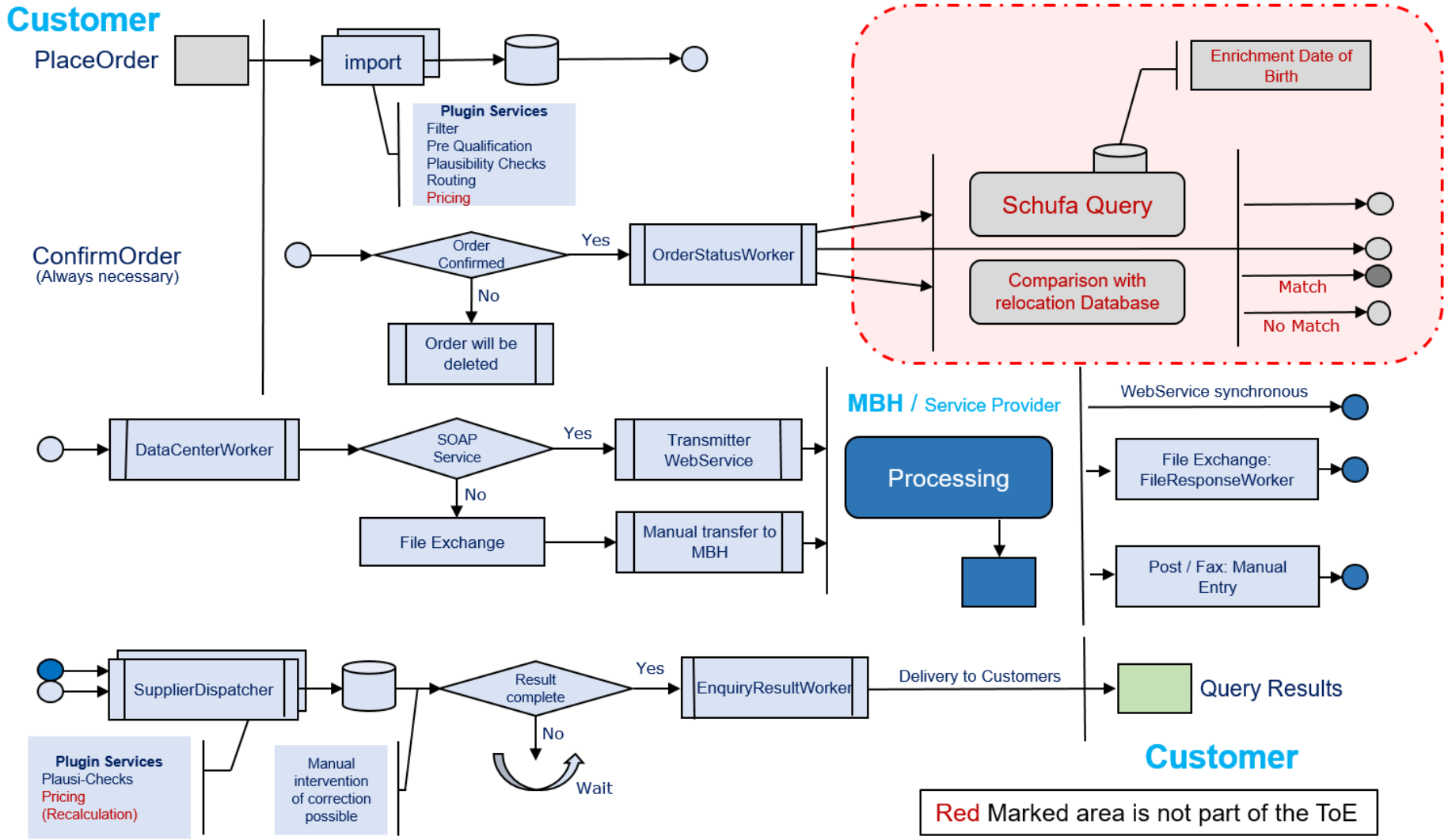

Fig 6: Data Flow Diagram

4. Requirement Profile

1. Requirements from a Legal Perspective	**Applicable or Not Applicable**
1.1.1. Record of processing activities	Applicable
1.1.2. Designation of a data protection officer	Applicable
1.1.3. Designation of a representative in the European Union	Not Applicable
1.1.4. Cooperation with the supervisory authority	Applicable
1.2.1. Existence of contractual clauses that meet all the requirements of Art. 28 GDPR (processor – principals)	Applicable
1.2.2. Implementation of the contractually agreed duties (processor – principals): Responsibilities, processes, work instructions	Applicable
1.3.1. Selection of other processors with regard to data protection guarantees	Applicable
1.3.2. Existence of signed data processing agreements with all other processors	Applicable
1.3.3. Implementation of the contractually agreed duties (processor – other processors): Responsibilities, processes, work instructions	Applicable
1.4.1. Statutory confidentiality obligations as well as professional secrets and special official secrets not based on statutory provisions	Not Applicable
1.4.2.1. Existence of an adequacy decision / appropriate safeguards	Applicable
1.4.2.2. Bound by instructions with regard to the transfer of personal data to third countries	Applicable
1.5.1. Data protection by design	Applicable
1.5.2. Data protection by default	Applicable
1.5.3. Provision of a data protection leaflet	Applicable
2. Technical and Organisational measures: Accompanying measures to protect the data subjects	**Applicable or Not Applicable**
2.1.1.1. Physical access control	Applicable
2.1.1.2. Access to portable media and mobile devices	Applicable
2.1.1.3. Access to data, programmes and devices	Applicable
2.1.1.4. Identification and authentication	Applicable
2.1.1.5. Use of passwords	Applicable
2.1.1.6. Organisation and documentation of access controls	Applicable
2.1.2.1. Logging mechanisms	Applicable
2.1.2.2. Operation of the logging mechanisms	Applicable
2.1.3. Network and transport security	Applicable
2.1.4.1. General Measures	Applicable
2.1.4.2. Back-up mechanisms	Applicable
2.1.4.3. Backup storage	Applicable
2.1.4.4. Recovery mechanisms	Applicable
2.1.5.1. Risk analysis	Applicable
2.1.5.2. Documentation of technical and organisational measures for data protection	Applicable
2.1.5.3. Documentation of individual obligations	Applicable
2.1.5.4. Inventory list of hardware, software, data and media	Applicable
2.1.5.5. Storage media management	Not Applicable
2.1.5.6. Instruction of employees; duty of confidentiality	Applicable
2.1.5.7. Data protection and security audits	Applicable
2.1.5.8. Incident management by processors	Applicable
2.1.5.9. Test and release	Applicable
2.1.6. Disposal and erasure of personal data	Applicable
2.1.7. Temporary files	Applicable
2.1.8. Documentation of the processing operations from the customer's point of view	Applicable
2.2.1. Encryption	Applicable

2.2.2. Pseudonymisation and Anonymisation	Applicable

3. Rights of the Data Subjects	**Applicable or Not Applicable**
3.1. Right to information	Applicable
3.2. Right of access	Applicable
3.3. Right to rectification	Applicable
3.4. Right to erasure	Applicable
3.5. Right to restriction of processing	Applicable
3.6. Right to data portability	Applicable
3.7. Right to object	Applicable

5. Overview of Evaluation Methods

5.1. Document Review

Legal Documents related to the ToE	
Document Type	**Remark**
Record of Processing Activities	OK
Certificate of appointment of the Data Protection Officer (DPO)	OK
Communication of DPO contact details to competent SA	OK
Work instructions re cooperation with competent supervisory authority	OK
Templates for Data Processing Agreements (DPA) between the processor and its principals (three templates in total)	OK
Work instruction re compliance with Art. 28 GDPR	OK
Signed data processing agreement/s (DPAs) with principals (sample of two agreements)	OK
Work instructions / process descriptions to ensure compliance with DPA clauses (processor - principal)	OK
List of other processors / sub-processors with ToE relevance and their locations	OK
Document re the selection of other processors in general	OK
Document/s demonstrating careful selection of each other processor	OK
Signed data protection agreement/s with other processors (DPA) (seven agreements)	OK
Work instructions / process descriptions to ensure compliance with DPA clauses (processor – other processors)	OK
Transfer Impact Assessments (TIA) regarding CH and UK	OK
Document/s re data protection by design and by default	OK

Technical Documents related to the ToE	
Document Type	**Remark**
Data Flow Diagram	OK
Documentation regarding Technical and Organisational Measures (TOMs)	OK
Log Data	OK
Evidences of relevant Certifications	OK
Evidences of relevant Audits / Pentest Results	OK
Information Security Policy	OK
Information Security Concept	OK

Other Documents related to the ToE	
Document Type	**Remark**
Information Sheets, User Manuals or Similar	OK

EuroPriSe specific Documents	
Document Type	**Remark**
Application for Certification	OK
ToE Description	OK
Results of Risk Analysis	OK
Results of Maturity Assessment	OK
Affirmation Declaration	OK
Data Protection Leaflet	OK

5.2. Remote Demonstration session

During the Remote demonstration session, RISER ID have explained the entire procedure of the RISER-Service that involves

- Authentication and authorization process of the RISER Internal Client
- Handling of Customer portal
- Log mechanism
- Processing of request and result data

Regarding the IT operations and management at the Data Centre, Ixsys GmbH have demonstrated the necessary topics like in particular:

- Incident Management
- Server Hardening and management
- Roles management
- Access control (physical and logical)

5.3. Interviews

After the analysis of the evidences shown during the remote demonstration session, evaluation team has organized an Interview session with same personnel to address questions on the following topics

- Overview of RISER Internal Client and Customer Portal
- Authentication methods on Internal Client and VPN (Virtual Private Network) to data centre
- Encryption techniques
- Logs management
- Backup and recovery
- Incidence Handling management
- Server hardening
- Network security

5.4. Use of Tools

SSLLabs was used for the evaluation purpose of the following criteria

- Network and Transport Security
- Encryption

6. Result

6.1 Result of Legal and Technical Evaluation

The overall result of the evaluation is "passed" (i.e. that the target of evaluation meets all applicable requirements from the EuroPriSe Criteria Catalogue for Processors (DE) v3.0).

_____

Place, Date Name of Lead Evaluator Signature

6.2 Result of Review of Evaluation Results

The review team has reviewed all information and results related to the evaluation. The review team shares the assessment of the evaluation team that all applicable requirements of the EuroPriSe criteria catalogue for processors (DE) v3.0 are met.

_____

Place, Date Name of Lead Reviewer Signature