EuroPriSe
European
Privacy Seal

European Privacy Seal
– *privacy at its best*

RISER-Dienst
Kurzgutachten

Versionshistorie

Version	Datum	Änderungsgrund	Autor(en)
1.0	28.11.2023	Initiale Version	Arghya Biswas
1.1	05.12.2023	Änderungen durch das Bewertungsteam	Sebastian Meissner
1.2	15.12.2023	Redaktionelle Änderungen aufgrund von Feedback seitens RISER ID Services GmbH	Sebastian Meissner

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Art der Zertifizierung und anzuwendende EuroPriSe-Vorgabedokumente

Art der Zertifizierung
Verarbeitungsvorgänge von Auftragsverarbeitern
Erstmalige Zertifizierung

Anwendbarer Kriterienkatalog
EuroPriSe-Kriterienkatalog für Verarbeitungsvorgänge von Auftragsverarbeitern (DE) v3.0

Anwendbare Verfahrensordnung
EuroPriSe-Verfahrensordnung für Verarbeitungsvorgänge von Auftragsverarbeitern v2.1

Anwendbares Evaluationskompendium
EuroPriSe-Kompendium der Evaluationsmethodik für Verarbeitungsvorgänge von Auftragsverarbeitern v2.1

Anwendbare Matrix der Evaluationsmethoden
Matrix zu Evaluationsarten und -methoden v2.1

2. Name des Zertifizierungskunden und allgemeine Informationen über diesen

Name des Zertifizierungskunden
RISER ID Services GmbH

Adresse des Zertifizierungskunden
Rudolfstr. 9
10245 Berlin
Deutschland

Zugehörigkeit zu einer Unternehmensgruppe
Ja. Deutsche Post Adress GmbH & Co. KG

Branche, in der der Zertifizierungskunde in erster Linie tätig ist
Öffentlicher Dienst und Geschäftskunden

3. Informationen zum Zertifizierungsgegenstand ("ToE-Beschreibung")

Name des Zertifizierungsgegenstands (Target of Evaluation – ToE)

RISER-Dienst

Beschreibung des Zertifizierungsgegenstands in Textform

Der RISER-Dienst (Registry Information Service on European Residents) ist ein von der RISER ID Services GmbH (nachfolgend: RISER ID) angebotener Dienst zur Beschaffung von Auskünften aus dem Melderegister im Auftrag von öffentlichen oder privaten Stellen. Über das Kundenportal https://kunde.riserid.eu/login.xhtml können diese Auskünfte aus den Melderegistern in Deutschland, der Schweiz und Österreich anfordern.

Anfragen über RISER-Dienst werden von RISER ID an die zuständigen Meldebehörden weitergeleitet und von diesen bearbeitet. Die Auskünfte aus dem Melderegister werden in der Regel elektronisch erteilt. Wo dies (noch) nicht möglich ist, werden Anfragen konventionell (per Brief oder Fax) gestellt.

Die aus den Anfragen gewonnenen Ergebnisdaten werden dem Anfragenden (RISER-Kunden) dann über RISER-Dienst zur Abholung zur Verfügung gestellt und unter Einhaltung der vertraglich vereinbarten Zeitspanne wieder gelöscht. Bei der Auskunftserteilung aus dem Melderegister verarbeitet RISER ID die Anfragedaten und die Ergebnisdaten mittels RISER-Dienst, indem sie die ein- und ausgehenden Daten auf Plausibilität prüft, Formatstrukturen anpasst und inkonsistente Ergebnisdaten ggf. manuell überprüft.

Die nachfolgende Abbildung gibt einen Überblick über den RISER-Dienst:

Abb. 1: Überblick über den RISER-Dienst

Um sich für das RISER-Kundenportal zu registrieren, müssen (künftige) Kunden zunächst die folgenden Daten angeben:

- Vor- und Nachname
- Name des Unternehmens oder der Institution
- E-Mail-Adresse
- Telefonnummer (optional)

Nach der Verarbeitung dieser Daten durch die Vertriebsabteilung von RISER ID erhält der Kunde die "Vereinbarung über die Nutzung des europäischen Registrierungsinformationsdienstes RISER". Sobald der Vertrag abgeschlossen ist, erhält der Kunde die Zugangsdaten (Kundenname, Benutzername und Passwort). Dazu wird ein Link (gültig für die nächsten 24 Stunden) an die E-Mail-Adresse des Kunden gesendet. Der Kunde nutzt den Link, um sich einzuloggen und sich ein neues Passwort zuzuweisen. Der erste Nutzer kann auch neue Benutzer anlegen oder bestehende Benutzer deaktivieren.

Registrierte Nutzer können Aufträge für amtliche Melderegisteranfragen erteilen.

Die Login-Seite des Kundenportals sieht wie folgt aus:

Abb. 2: Login-Seite des Kundenportals

Nach erfolgreichem Login können die Nutzer eine Einzelanfrage stellen, wie in der nachfolgenden Abbildung dargestellt:

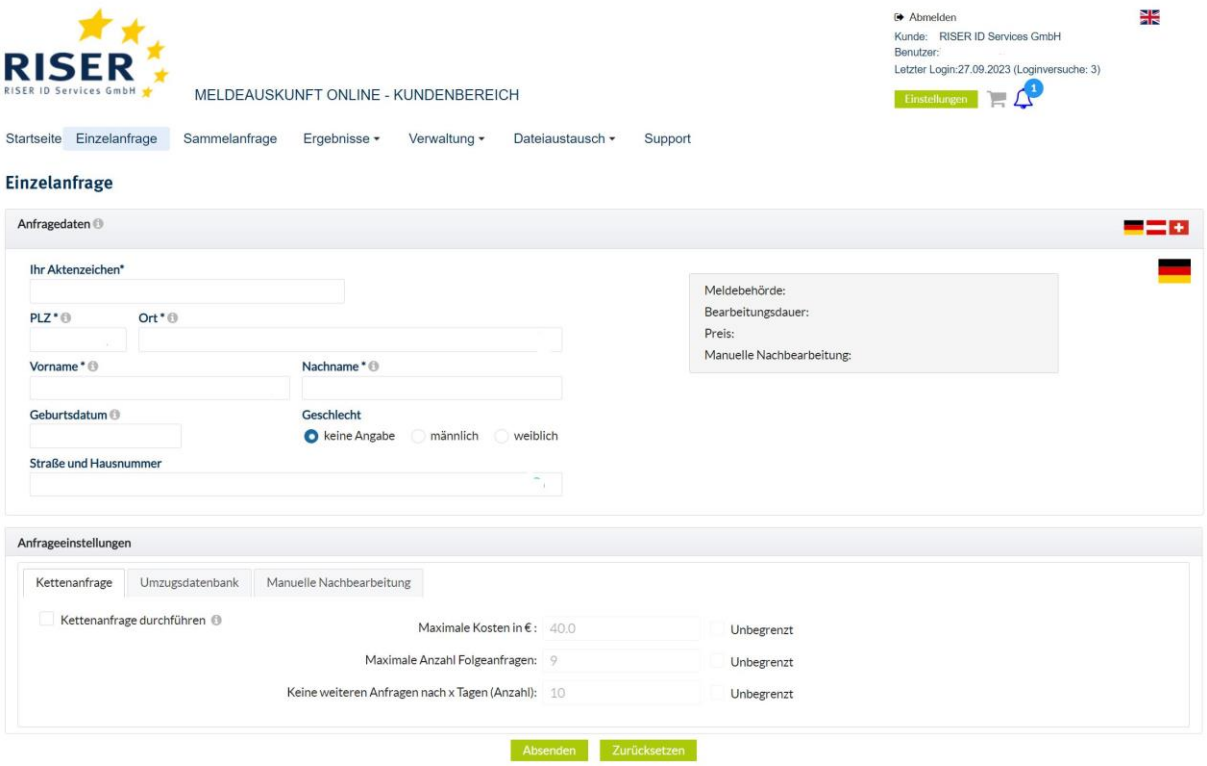

Abb. 3: RISER-Kundenportal: Einzelne Anfrage

Neben den Einzelanfragen kann der Kunde auch Großaufträge erteilen, indem er eine Liste von Aufträgen im Excel-Format hoch lädt.

Im Account erhält der Kunde eine Auflistung seiner gewünschten Aufträge, die Preisinformationen sowie die Aufforderung, diese zu bestätigen und somit den Auftrag zu erteilen. RISER ID verarbeitet den bestätigten Auftrag und stellt die Meldeergebnisse im Konto zur Verfügung. Die Auftragsübersicht eines Kunden ist nachfolgend abgebildet:

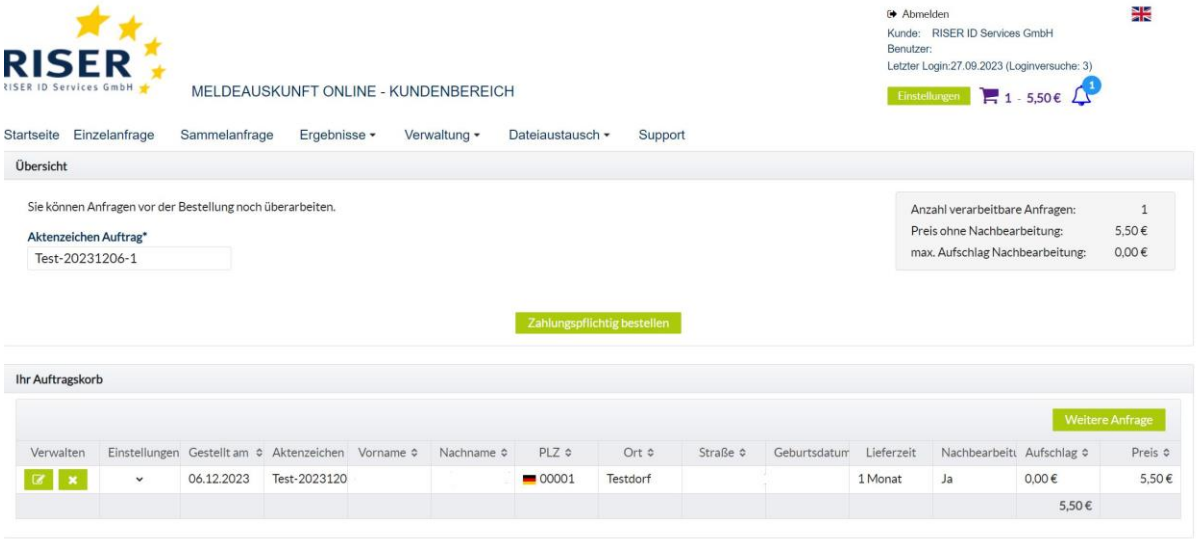

Abb. 4: Auftragsübersicht

Der Kunde kann im Kundenportal auch jederzeit den aktuellen Status erteilter Aufträge einsehen, wie nachfolgend abgebildet:

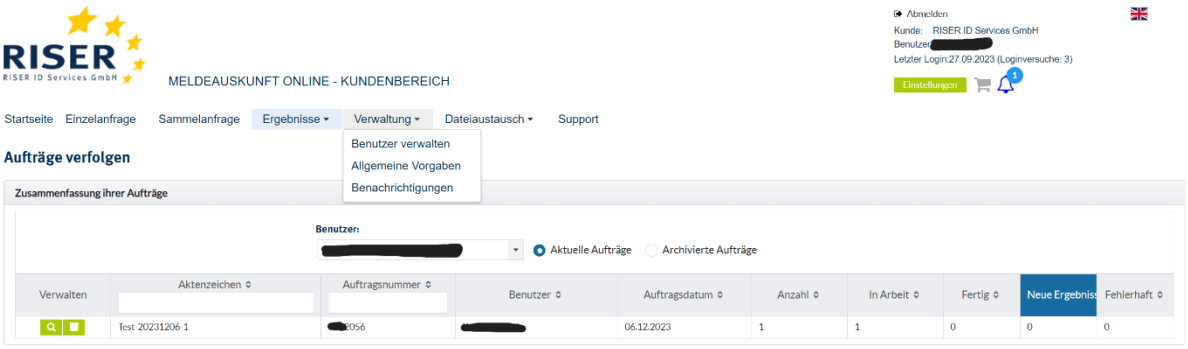

Abb. 5: Auftragsstatus

Der Prozess des RISER-Dienstes setzt sich aus den folgenden Schritten zusammen:

- Ein Kunde erteilt einen Auftrag zur Einholung von Auskünften aus dem Melderegister. Der RISER-Dienst prüft den eingegangenen Auftrag auf Vollständigkeit und ermittelt die zuständige Meldebehörde.
- Der Antrag wird in das jeweils gültige Format umgewandelt und an die Meldebehörde gesendet.
- Die Meldebehörde führt die Abfrage im Melderegister durch und übermittelt das Ergebnis an RISER-Dienst.
- RISER ID erhält das Ergebnis, prüft es und stellt es dem Kunden zur Abholung im Bereich "Ergebnisse" zur Verfügung.
- Der Kunde holt das Ergebnis ab.

Beschreibung der wichtigsten Aspekte des ToE

Verarbeitungsvorgänge, Prozesse & Funktionalitäten

Die nachfolgend aufgelisteten Prozesse und Funktionalitäten sind Bestandteil des ToE:

- Registrierung der Nutzer
- Grundfunktionen des RISER-Dienstes
  - Verarbeitung der Anfrage- und Ergebnisdaten
  - Authentifizierung der Nutzer beim Einloggen
  - Verarbeitung von Logdateien

Zweck(e)

- Der RISER-Dienst bietet vollen Zugang zu den Meldebehörden in Deutschland, den Personenstandsregistern in der Schweiz und dem zentralen

Personenstandsregister in Österreich. Die Kunden von RISER ID nutzen den Dienst für die Einholung von Melderegisterauskünften.

- Die Übermittlung von Anfragen und Ergebnissen zwischen Auftraggeber und RISER ID erfolgt auf elektronischem Wege. Wo RISER-Dienst nicht über eine elektronische Anbindung verfügt, werden die Anfragen konventionell (Brief, Fax) bearbeitet. Dies wird hauptsächlich von Unterauftragnehmern durchgeführt.

Kategorien von betroffenen Personen

Das ToE betrifft die folgenden Kategorien betroffener Personen:

- Personen, die im Melderegister eingetragen sind (Einwohner) und über die mittels RISER-Dienst Auskunft erteilt wird;
- Kunden und deren Mitarbeiter, die RISER-Dienst nutzen;
- Mitarbeiter von RISER ID, die die Aufträge bearbeiten.

Kategorien personenbezogener Daten

Die folgenden Kategorien personenbezogener Daten werden erhoben:

- Anfrage- und Ergebnisdaten
- Daten zur Benutzerregistrierung und -authentifizierung
- Logdaten

Im Zusammenhang mit Anfragen / Ergebnissen werden die folgenden Daten über die hiervon betroffenen Personen (Einwohner) verarbeitet:

- Vorname
- Nachname
- Geschlecht
- Geburtsdatum
- Postleitzahl
- Stadt
- Straße
- Hausnummer
- Ländercode (AT, CH, DE)

RISER Service verarbeitet keine besonderen Kategorien personenbezogener Daten.

Relevante Standorte

Es gibt mehrere Standorte, die für diesen Zertifizierungsgegenstand relevant sind:

- Der Support des operativen Geschäfts und die Weiterentwicklung des RISER-Dienstes und des Internal Client (Software nur für RISER-Mitarbeiter) erfolgt im Büro von RISER ID in Berlin. Die IT-Infrastruktur sowie die Office-Anwendungen im Berliner Büro werden im Rahmen der Aufgabenteilung innerhalb der

Unternehmensgruppe von der Deutsche Post Adress GmbH & Co. KG mit Sitz in Deutschland verwaltet.

- Die IT-Systeme von RISER ID befinden sich im Rechenzentrum der North C Group (früher bekannt als IP Exchange GmbH) in Deutschland. Hierbei handelt es sich um ein reines Housing.
- Der Betrieb der IT-Systeme von RISER ID wird durch die Ixsys EDV Systemberatung mit Sitz in Deutschland bereitgestellt.

Drittstaatentransfers

Der RISER-Dienst wird auch von in Drittstaaten ansässigen Kunden genutzt. Konkret handelt es sich (lediglich) um Kunden aus der Schweiz und aus Großbritannien.

Werden Anfragen an Meldebehörden in der Schweiz gestellt, übermittelt RISER ID die Anfragedaten an die jeweiligen Behörden. Darüber hinaus bedient sich RISER ID in diesem Fall eines Unterauftragsverarbeiters mit Sitz in der Schweiz.

Es kann bei der Verwendung von RISER-Dienst folglich zu Übermittlungen in die Schweiz und nach Großbritannien kommen.

Für beide Staaten gibt es Angemessenheitsbeschlüsse der Europäischen Kommission (Schweiz: 2000/518/EG; UK: (EU) 2021/1772), auf welche diese Drittstaatentransfers gestützt werden können.

Anwendungsbereich

Geschäftskunden, öffentlicher Dienst

Aussagekräftige grafische Darstellung des Datenflusses

Siehe Abbildung 6 weiter unten.

Verarbeitungsvorgänge, die Bestandteil des ToE sind

ToE ist der RISER-Dienst, bestehend aus den folgenden Bestandteilen:

- RISER Internal Client (Software nur für RISER-Mitarbeiter)
- RISER-Kundenportal
- Portale für Lieferanten und Meldebehörden (nur in Bezug auf die Verarbeitung von Abfrage- und Ergebnisdaten vom ToE umfasst)
- Registrierung und -authentifizierung
- Protokollierung (Logging)

Verarbeitungsvorgänge, die nicht Bestandteil des ToE sind

An dieser Stelle erfolgt eine tabellarische Auflistung aller Verarbeitungsvorgänge / Komponenten, die in engem Zusammenhang mit dem ToE stehen, aber nicht Bestandteil des ToE sind.

Vorliegend sind insbesondere Funktionalitäten, bei denen es sich nicht um Grundfunktionen des RISER-Dienstes handelt, sondern die nur auf besonderen Wunsch des Kunden zur Verfügung gestellt werden (optionale Funktionen), aus dem ToE ausgeschlossen worden.

Nicht Bestandteil des ToE sind:

- Die Nutzung von RISER-Dienst mittels Smartphones und Tablets;
- Die Einsatzumgebung in den Räumlichkeiten des Anwenders (RISER ID-Kunden);
- Die Einbeziehung der Umzugsdatenbank (optionale Funktion);
- Die Dienstleistung zur Anreicherung mit Geburtsdaten (erbracht durch die Schufa Holding AG) (optionale Funktion);
- Die Bearbeitung von Rückläufern (ReAdress) (optionale Funktion);
- Arbeitgeberidentifikation und Adressrecherche (optionale Funktion);
- Weitere Dienstleistungen von RISER ID;
- E-Mail-Verschlüsselungsgateway, da kein Austausch von personenbezogenen Daten erfolgt, die für das ToE relevant sind.

Aussagekräftige grafische Darstellung des Datenflusses:

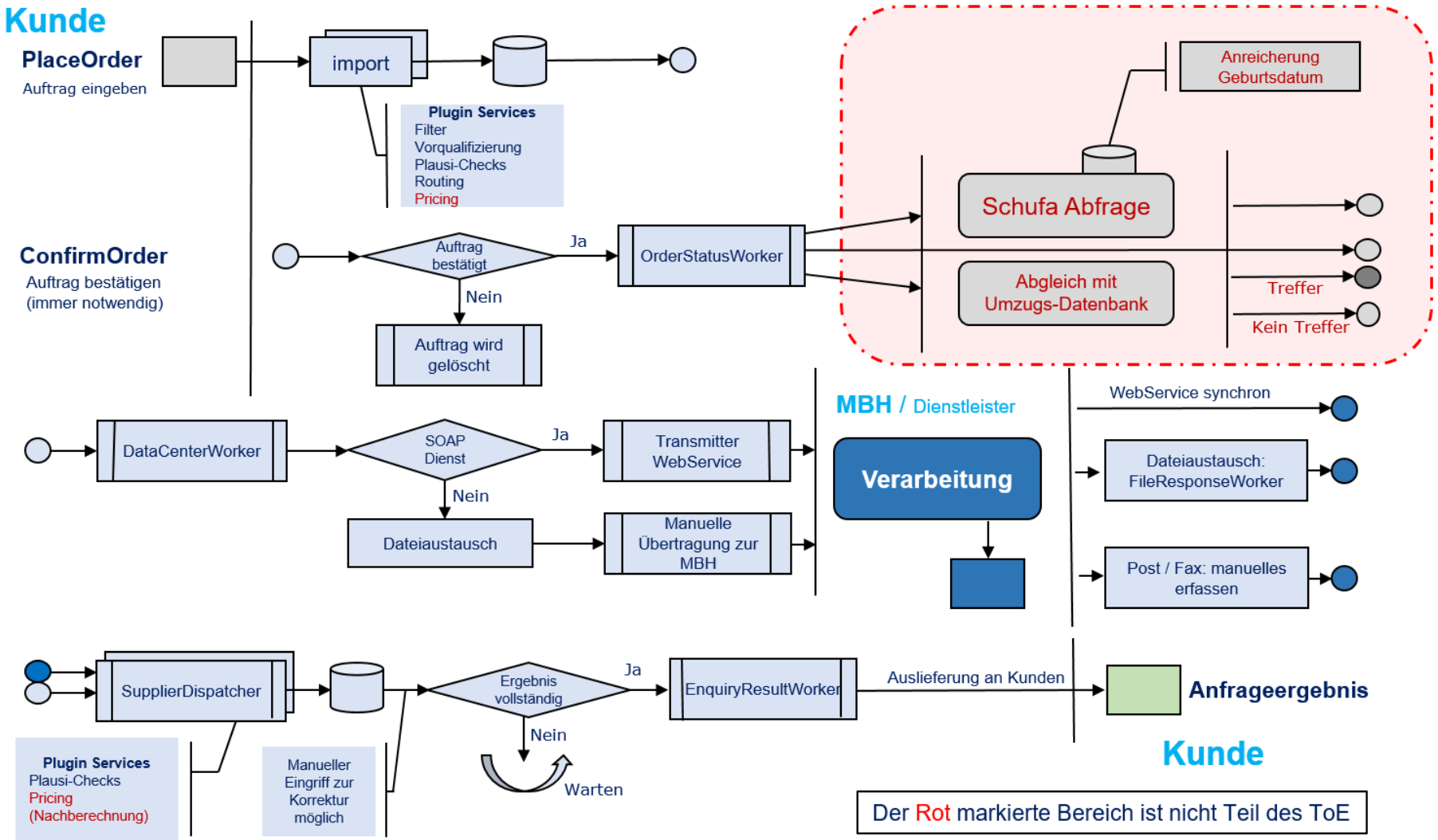

Abb. 6: Datenflussdiagramm

4. Anforderungsprofil

1. Anforderungen aus rechtlicher Sicht	**Anwendbar oder nicht anwendbar**
1.1.1. Verzeichnis der Verarbeitungstätigkeiten	Anwendbar
1.1.2. Benennung eines Datenschutzbeauftragten	Anwendbar
1.1.3. Benennung eines Vertreters in der Europäischen Union	Nicht anwendbar
1.1.4. Zusammenarbeit mit der Aufsichtsbehörde	Anwendbar
1.2.1. Vorhandensein von Vertragsklauseln, die alle Anforderungen des Art. 28 DSGVO erfüllen (Auftragsverarbeiter – Auftraggeber)	Anwendbar
1.2.2. Umsetzung der vertraglich vereinbarten Pflichten (Auftragsverarbeiter – Auftraggeber): Verantwortlichkeiten, Prozesse, Arbeitsanweisungen	Anwendbar
1.3.1. Auswahl weiterer Auftragsverarbeiter im Hinblick auf Garantien zur Wahrung des Datenschutzes	Anwendbar
1.3.2. Vorhandensein unterschriebener AV-Verträge mit allen weiteren Auftragsverarbeitern	Anwendbar
1.3.3. Umsetzung der vertraglich vereinbarten Pflichten (Auftragsverarbeiter – weiterer AV): Verantwortlichkeiten, Prozesse, Arbeitsanweisungen	Anwendbar
1.4.1. Gesetzliche Geheimhaltungspflichten sowie Berufsgeheimnisse und besondere Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen	Nicht anwendbar
1.4.2.1. Vorliegen eines Angemessenheitsbeschlusses / geeigneter Garantien	Anwendbar
1.4.2.2. Weisungsgebundenheit im Hinblick auf Übermittlung personenbezogener Daten in Drittländer	Anwendbar
1.5.1. Datenschutz durch Technikgestaltung	Anwendbar
1.5.2. Datenschutz durch datenschutzfreundliche Voreinstellungen	Anwendbar
1.5.3. Zurverfügungstellung eines Datenschutzmerkblatts	Anwendbar
2. Technische und organisatorische Maßnahmen: Begleitende Maßnahmen zum Schutz der betroffenen Person	**Anwendbar oder nicht anwendbar**
2.1.1.1. Kontrolle des physischen Zugangs (Zutritts)	Anwendbar
2.1.1.2. Zugang zu transportablen Medien und mobilen Geräten	Anwendbar
2.1.1.3. Zugang zu Daten, Programmen und Geräten	Anwendbar
2.1.1.4. Identifikation und Authentifizierung	Anwendbar
2.1.1.5. Nutzung von Passwörtern	Anwendbar
2.1.1.6. Organisation und Dokumentation von Zugangskontrollen	Anwendbar
2.1.2.1. Protokollierungsmechanismen (Loggingmechanismen)	Anwendbar
2.1.2.2. Betrieb der Protokollierungsmechanismen (Loggingmechanismen)	Anwendbar
2.1.3. Netzwerk- und Transportsicherheit	Anwendbar
2.1.4.1. Allgemeine Maßnahmen	Anwendbar
2.1.4.2. Sicherungsmechanismen (Backup)	Anwendbar
2.1.4.3. Speicherung von Sicherungskopien	Anwendbar
2.1.4.4. Wiederherstellungsmechanismen	Anwendbar
2.1.5.1. Risikoanalyse	Anwendbar
2.1.5.2. Dokumentation technischer und organisatorischer Maßnahmen zum Datenschutz	Anwendbar
2.1.5.3. Dokumentation individueller Verpflichtungen	Anwendbar
2.1.5.4. Inventarliste zu Hardware, Software, Daten und Medien	Anwendbar
2.1.5.5. Management von Speichermedien	Nicht anwendbar
2.1.5.6. Unterweisung der Mitarbeiter; Pflicht zur Verschwiegenheit	Anwendbar
2.1.5.7. Datenschutz- und Sicherheitsaudits	Anwendbar
2.1.5.8. Vorfallmanagement (Incident-Management) durch Auftragsverarbeiter	Anwendbar
2.1.5.9. Test und Freigabe	Anwendbar
2.1.6. Entsorgung und Löschung personenbezogener Daten	Anwendbar
2.1.7. Temporäre Dateien	Anwendbar
2.1.8. Dokumentation der Verarbeitungsvorgänge aus Kundensicht	Anwendbar
2.2.1. Verschlüsselung	Anwendbar
2.2.2. Pseudonymisierung und Anonymisierung	Anwendbar

3. Rechte der betroffenen Personen	Anwendbar oder nicht anwendbar
3.1. Recht auf Information	Anwendbar
3.2. Auskunftsrecht	Anwendbar
3.3. Recht auf Berichtigung	Anwendbar
3.4. Recht auf Löschung	Anwendbar
3.5. Recht auf Einschränkung der Verarbeitung	Anwendbar
3.6. Recht auf Datenübertragbarkeit	Anwendbar
3.7. Widerspruchsrecht	Anwendbar

5. Überblick über die Evaluationsmethoden

5.1. Dokumentenprüfung

Rechtliche Dokumente bezüglich des ToE	
Dokumententyp	**Ergebnis**
Verzeichnis von Verarbeitungstätigkeiten	OK
Bestellurkunde des Datenschutzbeauftragten (DSB)	OK
Mitteilung der Kontaktdaten des DSB an die zuständige Aufsichtsbehörde	OK
Arbeitsanweisung zur Zusammenarbeit mit der zuständigen Aufsichtsbehörde	OK
Vertragsmuster für Auftragsverarbeitungsverträge (AVV) des Auftragsverarbeiters mit seinen Auftraggebern (insgesamt drei Vertragsmuster)	OK
Arbeitsanweisung dazu, wie die Einhaltung von Art. 28 DSGVO sichergestellt wird	OK
Unterschriebene Auftragsverarbeitungsverträge (AVV) mit Auftraggebern (Stichprobe von zwei Verträgen)	OK
Arbeitsanweisungen / Verfahrensbeschreibungen zur Gewährleistung der Einhaltung der AVV-Klauseln (Auftragsverarbeiter - Auftraggeber)	OK
Liste der weiteren Auftragsverarbeiter (“Subs”) mit ToE-Relevanz und ihrer Standorte	OK
Dokument bezüglich der Auswahl weiterer Auftragsverarbeiter im Allgemeinen	OK
Dokument, das die sorgfältige Auswahl eines jeden weiteren Auftragsverarbeiters belegt	OK
Unterschriebene Auftragsverarbeitungsverträge (AVV) mit weiteren Auftragsverarbeitern („Subs“) (sieben Verträge)	OK
Arbeitsanweisungen / Prozessbeschreibungen zur Sicherstellung der Einhaltung der AVV-Klauseln (Auftragsverarbeiter - weitere Auftragsverarbeiter („Subs“))	OK
Transfer Impact Assessments (TIA) bzgl. CH und UK	OK
Dokument/e bezüglich Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	OK

Technische Dokumente bezüglich des ToE	
Dokumententyp	**Ergebnis**
Datenflussdiagramm	OK
Dokumentation der technischen und organisatorischen Maßnahmen (TOMs)	OK
Logdaten	OK
Nachweise über einschlägige Zertifizierungen	OK
Nachweise über relevante Audits / Pentest-Ergebnisse	OK
Informationssicherheitspolitik	OK
Informationssicherheitskonzept	OK

Andere Dokumente bzgl. des ToE	
Dokumententyp	**Ergebnis**
Informationsblätter, Benutzerhandbücher oder ähnliches	OK

EuroPriSe-spezifische Dokumente	
Dokumententyp	**Ergebnis**
Antrag auf Zertifizierung	OK
ToE-Beschreibung	OK
Ergebnisse der Risikoanalyse	OK
Ergebnisse der Reifegradbewertung	OK
Bestätigungserklärung	OK
Datenschutzmerkblatt	OK

5.2. Remote-Demonstrationssitzung

Während der Remote-Demonstrationssitzung hat RISER ID den gesamten Prozess des RISER-Dienstes erklärt, der Folgendes umfasst:

- Authentifizierungs- und Autorisierungsprozess des RISER Internal Client
- Handhabung des Kundenportals
- Log-Mechanismus
- Verarbeitung von Anfrage- und Ergebnisdaten

Für den IT-Betrieb und das Management im Rechenzentrum hat die Ixsys GmbH die notwendigen Themen dargestellt, wie insbesondere:

- Management von Zwischenfällen (Incident-Management)
- Server-Härtung (server hardening) und -verwaltung
- Verwaltung der Rollen (role management)
- Zugangskontrolle (physisch und logisch)

5.3. Interviews

Nach der Analyse der im Rahmen der Remote-Demonstrationssitzung gezeigten Nachweise hat das Evaluationsteam ein Gespräch mit demselben Personal organisiert, um Fragen zu folgenden Themen zu klären:

- Überblick über den RISER Internal Client und das Kundenportal
- Authentifizierungsmethoden auf dem Internal Client und für das VPN (Virtual Private Network) zum Rechenzentrum
- Verschlüsselungstechniken
- Protokoll- / Logs-Verwaltung
- Sicherung und Wiederherstellung
- Management von Zwischenfällen (Incident-Management)
- Server-Härtung
- Netzwerksicherheit

5.4. Nutzung von Tools

SSLLabs wurde für die Evaluation der folgenden Kriterien verwendet:

- Netzwerk- und Transportsicherheit
- Verschlüsselung

6. Ergebnis

6.1 Ergebnis der rechtlichen und technischen Evaluation

Das Gesamtergebnis der Evaluation ist "bestanden" (d.h. der Zertifizierungsgegenstand erfüllt alle anwendbaren Anforderungen des EuroPriSe-Kriterienkatalogs für Auftragsverarbeiter (DE) v3.0).

Arghya Biswas

Digitally signed by Arghya Biswas
DN: cn=Arghya Biswas, o=EuroPriSe Cert GmbH, ou=EuroPriSe CA, email=arghya.biswas@euprivacyseal.com, c=DE
Date: 2023.12.19 12:22:18 +01'00'

Ort, Datum	Name des Lead-Evaluators	Unterschrift

6.2 Ergebnis der Bewertung der Evaluationsergebnisse

Das Bewertungsteam hat alle Informationen und Ergebnisse im Zusammenhang mit der Evaluation überprüft. Das Bewertungsteam teilt die Einschätzung des Evaluationsteams, dass alle anwendbaren Anforderungen des EuroPriSe-Kriterienkatalogs für Auftragsverarbeiter (DE) v3.0 erfüllt sind.

Sebastian Meissner

Digitally signed by Sebastian Meissner
DN: cn=Sebastian Meissner, o=EuroPriSe Cert GmbH, ou=EuroPriSe CA, email=sebastian.meissner@euprivacyseal.com, c=DE
Date: 2023.12.19 14:49:32 +01'00'

Ort, Datum	Name des Lead-Bewerters	Unterschrift