Short Public Report

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

Vers.diagnose, Stand Februar 2023

2. Provider of the IT-based service:

Company Name:

Versdiagnose GmbH[1]

Address:

Prinzenstraße 16

30159 Hannover

Contact Person:

Herr Kay Pitzschel

[1] Im Folgenden: Versdiagnose.

3. Time frame of evaluation:

November 2020 – Februar 2023

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

Name of the Legal Expert:

Herr Jörg Schließke

Address of the Legal Expert:

TÜV Informationstechnik GmbH, Am TÜV 1, 45307 Essen, Germany

Name of the Technical Expert:

Herr Tobias Mielke

Address of the Technical Expert:

TÜV Informationstechnik GmbH, Am TÜV 1, 45307 Essen, Germany

5. Certification Authority:

Name: EuroPriSe Certification Authority
Address: Joseph-Schumpeter-Allee 25, 53227 Bonn, Deutschland
eMail: contact@euprivacyseal.com

6. Specification of Target of Evaluation (ToE):

Der ToE umfasst:

- Registrierung des Vermittlers
- Anmeldung des Vermittlers über die Website
- Risikoprüfung und Quick Check
- Ergebnisübersicht
- Interface: Datenübermittlung an Versicherer für manuelle Risikoprüfung
- Protokollerstellung
- Interface: Weitergabe der Berechnungsparameter an Versicherung zur Tarifberechnung
- Vertragsgestaltung
- Übermittlung der Dokumente
- technische Infrastruktur zur Durchführung der Risikoprüfung
- Website https://www.versdiagnose.de/~homepage/main.do

Der ToE umfasst **nicht**:

- die Verarbeitung der personenbezogenen Daten der Vermittler im CRM System

- elektronische Unterschrift (nepatec)
- Manuelle Risikoprüfung durch die angebundenen Versicherungsgesellschaften
- technische Infrastruktur der Vermittler und Versicherungsunternehmen
- Editor zum Einstellung der relevanten Fragen der Risikoüberprüfung
- Newsletter
- Fragen zur Risikoüberprüfung

7. General description of the IT product or IT-based service:

Die Applikation vers.diagnose ist eine rein weborientierte Plattform zur onlinebasierten Risikoprüfung und wird über die Webseite https://www.versdiagnose.de/ oder per Schnittstelle aufgerufen. Versicherungsvermittler können sich jederzeit anmelden und werden nach Prüfung kostenfrei registriert.

Die Plattform soll einen konsistenten Beratungsprozess ohne Medienbruch – von der Bedarfsermittlung über Produktauswahl, verbindliche Risikoprüfung und -bewertung bis hin zum Antrag mit elektronischer Unterschrift für Versicherungsinteressenten anbieten. Grundlage der Risikoprüfung ist ein für alle teilnehmenden Versicherer einheitlicher, reflexiver Fragenkatalog. Auf Grundlage dieser Angaben wird automatisch eine Risikoprüfungsentscheidung für die ausgewählten Produktbereiche ermittelt.

Über die Applikation ermittelt der Versicherungsvermittler (Lizenznehmer der versdiagnose GmbH) mit dem Interessenten zusammen die Möglichkeiten der Absicherung über den Abschluss einer Berufsunfähigkeits-, Grundfähigkeits-, Erwerbsunfähigkeits- oder Risikolebensversicherung. Hierbei werden zunächst die relevanten Daten für eine Risikoprüfung eingegeben, hierzu zählen:

<u>Angaben zur Person:</u>

- Geschlecht
- Geburtsdatum
- Größe
- Gewicht
- Angaben über Raucherstatus

<u>Angaben zum Beruf:</u>

- Berufsbezeichnung
- Berufsstatus
- Höchster Bildungsabschluss
- Tätigkeitsstatus
- Anzahl der Personalverantwortung
- Anteil körperlicher Arbeit
- Reisetätigkeit
- Brutto- / Nettojahreseinkommen

Als weitere Daten werden abgefragt, wie hoch die Rente bei Arbeitskraftverlust und das Kapital angesetzt werden, sowie in Folge eine Abfrage der Vorversicherung mittels „ja/nein“-Auswahl.

Anschließend werden vom Interessenten die Informationen zur Einschätzung der Sonderrisiken (Gefahren im Beruf/ Gefahren bei Sport oder Hobby), sowie Konkretisierung der Versicherungsanträge /-verträge bei anderen Gesellschaften erfragt und durch den Vermittler eingegeben.

Zum Abschluss erfolgen die Gesundheitsfragen, welche durch einen effektiven Aufbau ermöglichen, das „Risiko“ des Versicherers bei Vertragsübernahme des Interessenten in den meisten Fällen soweit einschätzen zu können, dass keine weitere Nachfassung oder Ergänzung notwendig ist.

Für den Fall, dass automatisch keine Risikoprüfungsentscheidung ermittelt werden kann, hat der Versicherer die Möglichkeit manuell eine Einschätzung einzutragen.

Versdiagnose stellt die Plattform für Versicherungsvermittler als Auftragsverarbeiter bereit. Versicherungsvermittler sind für die eigentliche Vermittlungs- bzw. Beratungsleistung zuständig, sodass die Verantwortung für das Vermittlungs- und Beratungsgeschäft bei den Versicherungsvermittlern als Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO liegt. Die fb research GmbH wird als Unterauftragsverarbeiterin gegenüber den Lizenznehmern eingesetzt.

8. Transnational issues:

Der Service Vers.diagnose wird derzeit nur in Deutschland angeboten. Es findet keine Datenübermittlung in Drittländer statt.

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

Vers.diagnose wird auf einer webbasierten Plattform zur Verfügung gestellt und ist über die Webseite https://www.versdiagnose.de/ oder per Schnittstelle aufrufbar. Es werden verschiedene Komponenten für die Realisierung der Risikoüberprüfung eingesetzt und im Rahmen der Zertifizierung betrachtet. Hierzu zählt die webbasierte Plattform für Versicherungsvermittler (Server, Netzwerkkomponenten, Speicherung) sowie die dafür erforderliche Software (Operatives System, Datenbank, Application Software, Web Interfaces).

Die Betriebssysteme und Datenbanken selbst werden nicht zertifiziert, sondern nur die Prozesse, die zur Erbringung der IT-gestützten Dienstleistung unter Verwendung dieser Komponenten erforderlich sind.

10. Edition of EuroPriSe Criteria used for the evaluation:

Criteria from January 2017

Commentary from May 2017

11. Evaluation methods:

- Durchsicht der von Versdiagnose GmbH zur Verfügung gestellten Dokumente, z.B. Datenschutzerklärung, Richtlinien, Auftragsverarbeitungsvertrag, Verzeichnis von Verarbeitungstätigkeiten, Prozessbeschreibungen, Nutzungsvertrag etc.)
- Analyse der Website www.versdiagnose.de/
- Interview mit dem Datenschutzbeauftragten und der Geschäftsführung
- Die technische Prüfung beinhaltet Folgendes:

  - Web Applikation OWASP testing guide (Web and API Top 10)

  - Port und Schwachstellenscan gegen erreichbare Dienste

  - SSL/TLS Scan

  - Mandantentrennung

  - Logging Überprüfung

  - Brute Force Angriff

  - Benutzerübergriffe prüfen

  - Passwort handling

  - Schnittstellenüberprüfung

  - Konfigurationsanalyse Systeme (u.a. Patch Management etc.)

  - Berechtigungskonzept

  - Verschlüsselungsmechanismen und Umsetzung

  - Dokumentenaudit der technischen Dokumentation

  - Überprüfung der Anonymisierung

  - Löschung von Daten

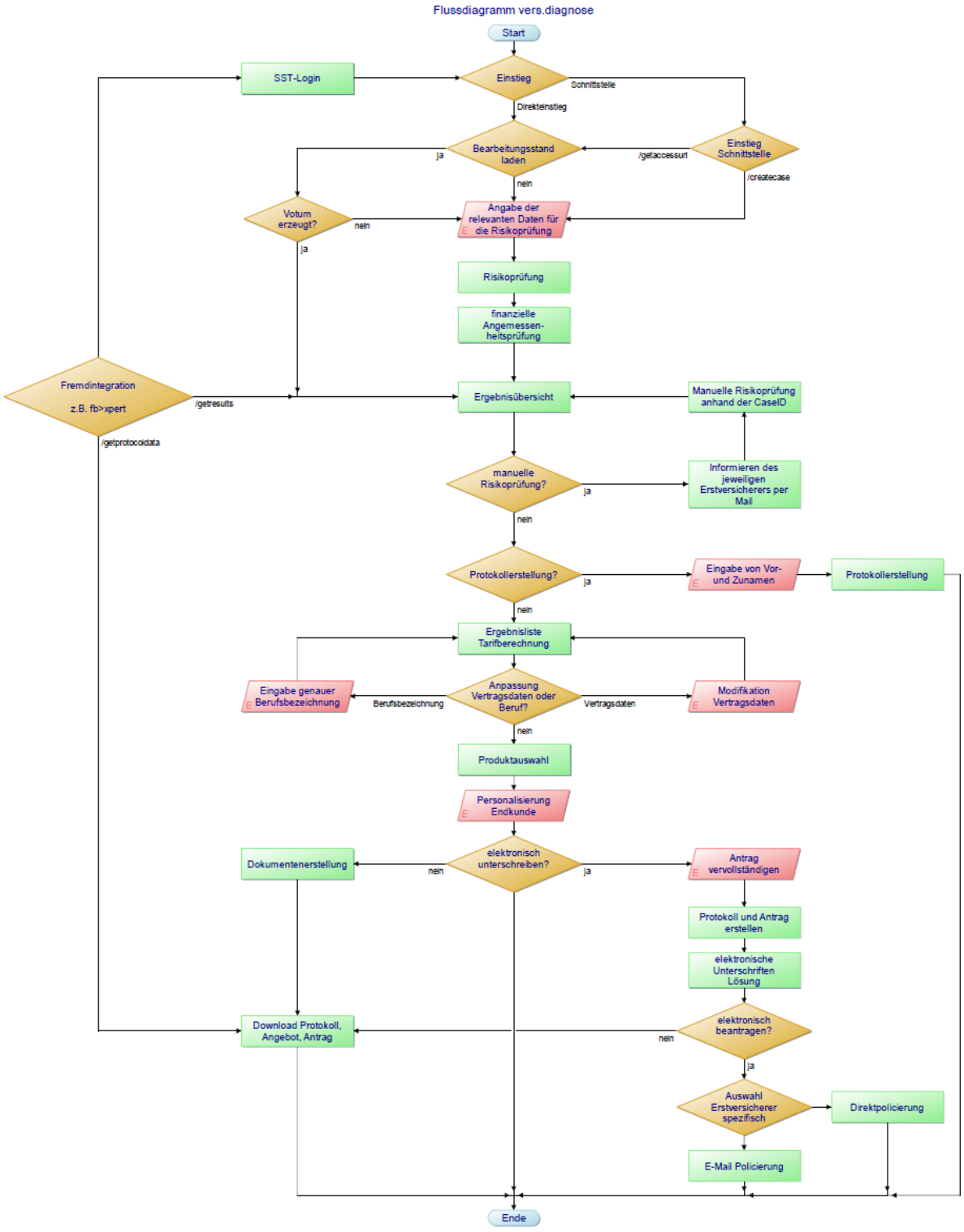
- On-Site/Remote Audit RZ und versdiagnose

12. Evaluation results:

Das Gesamtergebnis der Begutachtung ist wie folgt:

#	Set	Requirement	Evaluation result
1	1.2	Fundamental Technical Construction	adequate
2	2.1	Legal Basis for the Processing of Personal Data	Processing fully permitted
3	2.2	General Requirements	adequate
4	2.3	Special Requirements to the Various Phases of the Processing	adequate
5	2.4	Special Types of Processing Operations	adequate
6	2.5	Compliance with General Data Protection Principles	adequate
7	3.1	General duties	adequate
8	3.2	Technology-specific and Service-specific Requirements	adequate
9	4.1	Rights under the General Data Protection Regulation (GDPR)	adequate
10	4.2	Rights under the ePrivacy Directive (ePD)	Not applicable

13. Data flow:


Flussdiagramm vers.diagnose
Start
SST-Login
Einstieg
Schnittstelle
Direkteinstieg
Bearbeitungsstand laden
ja
/getaccessurl
Einstieg Schnittstelle
/createcase
nein
Votum erzeugt?
nein
ja
Angabe der relevanten Daten für die Risikoprüfung
Risikoprüfung
finanzielle Angemessen-heitsprüfung
Fremdintegration
z.B. fb>xpert
/getresults
/getprotocoldata
Ergebnisübersicht
Manuelle Risikoprüfung anhand der CaseID
manuelle Risikoprüfung?
ja
Informieren des jeweiligen Erstversicherers per Mail
nein
Protokollerstellung?
ja
Eingabe von Vor- und Zunamen
Protokollerstellung
nein
Ergebnisliste Tarifberechnung
Eingabe genauer Berufsbezeichnung
Berufsbezeichnung
Anpassung Vertragsdaten oder Beruf?
Vertragsdaten
Modifikation Vertragsdaten
nein
Produktauswahl
Personalisierung Endkunde
Dokumentenerstellung
nein
elektronisch unterschreiben?
ja
Antrag vervollständigen
Protokoll und Antrag erstellen
elektronische Unterschriften Lösung
Download Protokoll, Angebot, Antrag
nein
elektronisch beantragen?
ja
Auswahl Erstversicherer spezifisch
Direktpolicierung
E-Mail Policierung
Ende

14. Privacy-enhancing functionalities:

Die Anwendung vers.diagnose ist in einer Art ausgestaltet, die es ermöglicht, anhand eines Fragenkatalogs Risiken zu ermitteln und Versicherungstarife darzustellen ohne direkt personenbezogene Daten zu Versicherungsinteressenten vorab zu verarbeiten. Solange keine Antragstellung für einen Versicherungstarif erfolgt, werden Angaben von Betroffenen ohne Erhebung eines Namens oder sonstiger personenbezogenen Daten für die Risikoprüfung und Erstellung von Voten verwendet. Damit ein Versicherungsvermittler einen Fall wiedererkennen und aufrufen kann, wird jeder Fall mit einer Risikoprüfnummer (Case-ID) versehen. Aufgrund des Umstands, dass die Versdiagnose im Rahmen der Risikoüberprüfung nur die Case-ID und die dazu jeweiligen Angaben aus dem Fragenkatalog für eine Dauer von max. acht Wochen speichert, liegen die Datensätze in der Anwendung in diesem Zeitraum in pseudonymisierter Form vor. Es ist jedoch anzumerken, dass nach Ansicht der Zertifizierungsstelle jedoch angenommen werden kann, dass durch einzelne zusammenhängende Angaben unter bestimmten Umständen ein Personenbezug hergestellt werden kann und die Angaben damit nicht zwangsläufig pseudonym sind. Dies kann beispielsweise angenommen werden, wenn die Angaben der Person durch ihr seltenes Vorkommen hervorheben und die Angaben damit einzigartig machen. Ungeachtet dessen, ist in dieser Phase eine Eingabe von direkt personenbezogenen Daten weder erforderlich noch möglich. Durch das Setzen minimaler Berechtigungen ist ein unberechtigter Zugriff nahezu ausgeschlossen. Ferner werden alle Daten entsprechend verschlüsselt.

15. Issues demanding special user attention:

Keine

16. Compensation of weaknesses:

Nicht anwendbar

17. Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	adequate	Bis zur Antragstellung sind die Angaben, die vom Betroffenen erfragt werden auf das notwendige und unbedingt erforderliche Maß zum Zwecke der Tarifierung beschränkt und ohne Personenbezug. Im System werden gespeicherte Angaben aus einer Risikoprüfung bis zu acht Wochen pseudonymisiert durch Kennzeichnung mittels einer Case-ID vorgehalten.
Transparency	adequate	Die Datenschutzerklärung auf der Website folgt einer klaren Struktur, ist leicht verständlich und ist sowohl von der Startseite als auch von allen Unterseiten aus mit nur einem Klick aufrufbar. Es erfolgt der Hinweis, dass die Lizenznehmer für die Einhaltung der erforderlichen Transparenz hinsichtlich der Datenverarbeitung im Zuge der Risikoüberprüfung verantwortlich sind.
Technical-Organisational Measures	adequate	In den Front- und Backends werden keine personenbezogenen Daten zu den Interessenten vorgehalten. Ferner werden die IT-Systeme angemessen verschlüsselt. Die Anwendung ist mandantenfähig, d.h. kann das Software-System von mehreren Parteien genutzt werden, ohne dass ein gegenseitiger Einblick in die Daten der anderen Partei gewährt wird. Die Administration des Systems ist vom operativen Geschäft getrennt, so dass kein Zugriff auf die Kundendaten möglich ist.
Data Subjects' Rights	adequate	Sofern sich Betroffene in Bezug auf die Datenverarbeitung im Rahmen der Anwendung vers.diagnose direkt an die Versdiagnose wenden, verweist Versdiagnose auf die Verantwortlichkeit des Lizenznehmers und informiert den Lizenznehmer unverzüglich über die entsprechende Anfrage, damit diese in der vorgesehenen Frist bearbeitet werden kann.

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.

Essen, 03.03.2023	Jörg Schließke	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Essen, 03.03.2023	Tobias Mielke	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Certification 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 product or service in a way compliant with European regulations on privacy and data protection.

Place, Date	Name of Certification Authority	Signature