EuroPriSe European Privacy Seal

Short Public Report

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

Vers.diagnose, as of February 2023

2. Provider of the IT-based service:

Company Name:

Versdiagnose GmbH[1]

Address:

Prinzenstraße 16

30159 Hanover

Contact Person:

Mr Kay Pitzschel

[1] Hereafter: Versdiagnose.

3. Time frame of evaluation:

November 2020 - February 2023

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

Name of the Legal Expert:

Mr Jörg Schlißke

Address of the Legal Expert:

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

Name of the Technical Expert:

Mr 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, Germany
eMail: contact@euprivacyseal.com

6. Specification of Target of Evaluation (ToE):

The ToE includes:

- Registration of the insurance intermediary
- Registration of the insurance intermediary via the website
- Risk assessment and quick check
- Result overview
- Interface: Data transmission to insurer for manual risk assessment
- Protocol creation
- Interface: Passing on the calculation parameters to the insurance company for tariff calculation
- Contract design
- Transmission of the documents
- Technical infrastructure for carrying out the risk assessment
- Website https://www.versdiagnose.de/~homepage/main.do

The ToE does **not** include:

- the processing of the insurance intermediaries' personal data in the CRM system

- Electronic signature (nepatec)
- Manual risk assessment by the affiliated insurance companies
- Technical infrastructure of insurance intermediaries and insurance companies
- Editor for setting the relevant risk review questions
- Newsletter
- Risk review questions

7. General description of the IT-based service:

The vers.diagnose application is a purely web-oriented platform for online-based risk assessment and is accessed via the website https://www.versdiagnose.de/ or via interface. Insurance intermediaries can register at any time and are registered free of charge after verification.

The platform is intended to offer a consistent advisory process without media discontinuity - from needs assessment, product selection, binding risk assessment and evaluation to the application with electronic signature for prospective insurers. The basis of the risk assessment is a reflexive questionnaire that is uniform for all participating insurers. Based on this information, a risk assessment decision is automatically determined for the selected product areas.

Via the application, the insurance intermediary (licensee of versdiagnose GmbH) determines together with the interested party the possibilities of coverage by taking out an occupational disability-, basic disability-, disability or term life insurance. First, the relevant data for a risk assessment is entered, including:

Personal details:

- Gender
- Date of birth
- Size
- Weight
- Information on smoking status

Occupation details:

- Job title
- Occupational status
- Highest educational attainment
- Activity status
- Number of personnel responsibilities
- Proportion of physical work
- Travel
- Gross / net annual income

Further data requested are the amount of the annuity in the event of loss of working capacity and the capital, as well as a query on the previous insurance by means of a "yes/no" selection.

Subsequently, the interested party is asked for information on the assessment of special risks (occupational hazards / hazards in sports or hobbies), as well as concretisation of the insurance applications / contracts with other companies and entered by the insurance intermediary.

Finally, there are the health questions, which, due to their effective structure, enable the insurer to assess the "risk" of the interested party in most cases so far that no further amendment or supplement is necessary.

In the event that no underwriting decision can be determined automatically, the insurer has the option to manually enter an assessment.

Versdiagnose provides the platform for insurance intermediaries as a processor. Insurance intermediaries are responsible for the actual brokerage or advisory service, so that the responsibility for the brokerage and advisory business lies with the insurance intermediaries as data controllers within the meaning of Art. 4 No. 7 GDPR. fb research GmbH is used as a subcontracted processor vis-à-vis the licensees.

8. Transnational issues:

The Vers.diagnose service is currently only offered in Germany. There is no data transfer to third countries.

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

Vers.diagnose is provided on a web-based platform and can be accessed via the website https://www.versdiagnose.de/ or via interface. Various components are used for the realisation of the risk check and are considered within the scope of the certification. These include the web-based platform for insurance intermediaries (server, network components, storage) as well as the software required for this (operational system, database, application software, web interfaces).

The operating systems and databases themselves are not certified, but only the processes required to provide the IT-based service using these components.

10. Edition of EuroPriSe Criteria used for the evaluation:

Criteria from January 2017

Commentary from May 2017

11. Evaluation methods:

- Review of the documents provided by Versdiagnose, e.g. privacy policy, guidelines, order processing contract, directory of processing activities, process descriptions, user contract, etc.).
- Analysis of the website www.versdiagnose.de/
- Interview with the data protection officer and the management
- The technical examination includes the following:

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

  - Port and vulnerability scan against reachable services

  - SSL/TLS Scan

  - client separation

  - Logging Review

  - Brute Force Attack

  - Check user assaults

  - Password handling

  - interface verification

  - Configuration analysis of systems (including patch management, etc.)

  - authorisation concept

  - Encryption mechanisms and implementation

  - Document audit of the technical documentation

  - Verification of anonymisation

  - Data deletion

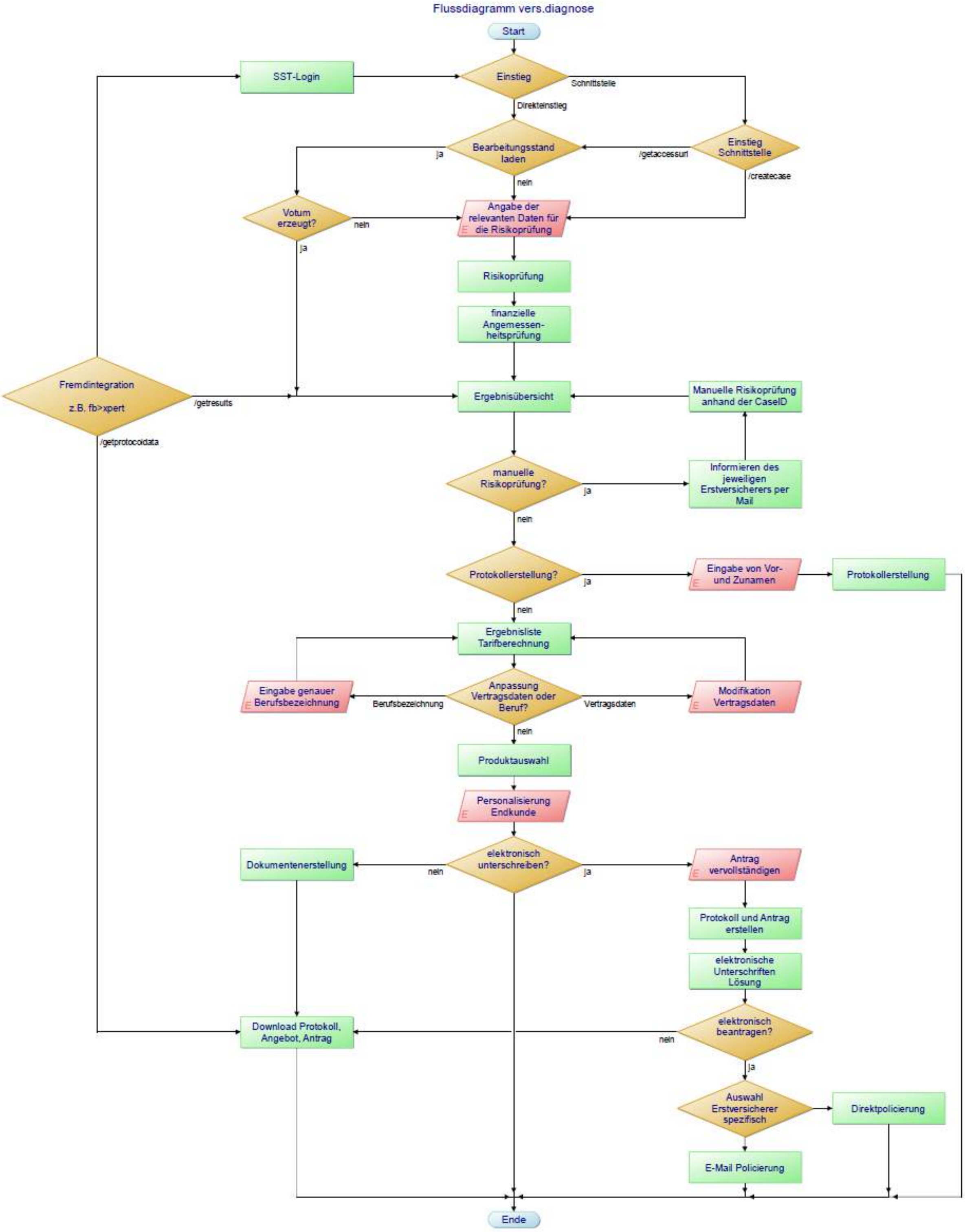
  - On-Site/Remote Audit RZ and versdiagnose

12. Evaluation results:

The overall result of the assessment is as follows:

#	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
Angabe der relevanten Daten für die Risikoprüfung
E
ja
Risikoprüfung
finanzielle Angemessen-heitsprüfung
Fremdintegration
z.B. fb>xpert
/getresults
Ergebnisübersicht
Manuelle Risikoprüfung anhand der CaseID
/getprotocoldata
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:

The vers.diagnose application is designed in a way that makes it possible to determine risks and present insurance tariffs on the basis of a catalogue of questions without directly processing personal data on prospective insurers in advance. As long as no application for an insurance tariff is made, information from data subjects is used without collecting a name or other personal data for the risk assessment and creation of votes. In order for an insurance intermediary to be able to recognise and call up a case, each case is assigned a risk assessment number (case ID). Due to the fact, that Versdiagnose only stores the case ID and the respective information from the questionnaire for a maximum of eight weeks in the context of the risk check, the data records in the application are available in pseudonymised form during this period. It should be noted, however, that in the opinion of the certification body it can be assumed that under certain circumstances a personal reference can be established through individual related details and the details are therefore not necessarily pseudonymous. This can be assumed, for example, if the details of the person stand out due to their rare occurrence and thus make the details unique. Regardless of this, it is neither necessary nor possible to enter directly personal data in this phase. By setting minimal authorisations, unauthorised access is almost impossible. Furthermore, all data is encrypted accordingly.

15. Issues demanding special user attention:

None

16. Compensation of weaknesses:

Not applicable

17. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	adequate	Until the application is submitted, the information requested from the person concerned is limited to what is necessary and absolutely required for the purpose of pricing and has no personal reference. The information stored in the system from a risk assessment is kept pseudonymised for up to eight weeks by means of a case ID.
Transparency	adequate	The privacy policy on the website follows a clear structure, is easy to understand and can be accessed from the homepage as well as from all sub-pages with just one click. It is pointed out that the licensees are responsible for complying with the required transparency regarding data processing in the course of the risk assessment.
Technical-Organisational Measures	adequate	No personal data on interested parties is kept in the front and back ends. Furthermore, the IT systems are appropriately encrypted. The application is multi-client capable, i.e. the software system can be used by several parties without granting mutual insight into each other's data. The administration of the system is separated from the operational business so that no access to client data is possible.
Data Subjects' Rights	adequate	Insofar as data subjects contact Versdiagnose directly with regard to data processing within the scope of the vers.diagnose application, Versdiagnose shall refer to the responsibility of the licensee and inform the licensee without delay of the corresponding request so that it can be processed within the stipulated period.

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 Schlißke

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