Short Public Report

1. Name and version of the IT product:

   OPEN/PROSOZ, v.2019.1.0.

2. Manufacturer or vendor of the IT product:

   Company Name: *PROSOZ Herten GmbH*

   Address: *Ewaldstraße 261, 45699 Herten, Germany*

   Contact Person: *Frank Jüttner, E-Mail: f.juettner@prosoz.de*

3. Time frame of evaluation:

   2019-10-04 – 2019-12-02.

4. EuroPriSe Experts who evaluated the IT product:

   Name of the Legal Expert: *Dr. Irene Karper*

   Address of the Legal Expert: *c/o datenschutz cert GmbH, Konsul-Smidt-Str. 88a, 28217 Bremen, Germany*

   Name of the Technical Expert: *Dr. Irene Karper*

   Address of the Technical Expert: *c/o datenschutz cert GmbH, Konsul-Smidt- Str. 88a, 28217 Bremen, Germany*

5. Certification Body:

   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):

Target of evaluation is the IT product OPEN/PROSOZ with the following modules:

- *Global claims processing (OPEN/PROSOZ Global)*
- *system administration (OPEN/PROSOZ System) with the Dialog Editor*
- *case-by-case handling (OPEN/PROSOZ Client).*

However, other offers or products of PROSOZ Herten GmbH are not part of the ToE. The website http://www.prosoz.de and other websites of PROSOZ Herten GmbH also are not part of the ToE. Processing by a processor according to Art. 28 GDPR by PROSOZ Herten GmbH is not included in the standard scope of OPEN/PROSOZ and is, therefore, not subject to evaluation. The ToE does neither include other support services with regard to anonymizing data records. The subject of the audit shall also not include the user's operating environment, its operating systems, the individual configuration of dialog boxes in OPEN/PROSOZ at the user's as well as tools used by the user for exchanging data or converting ASCII files to XML.

7. General description of the IT product:

OPEN/PROSOZ is a database-driven IT dialogue system used by social welfare institutions. The software supports the processing of social assistance benefits. The focus lies on the individual case processing of benefits according to the German Social Security Code (SGB) II, SGB XII or SGB IX. In addition, OPEN/PROSOZ enables the processing of requirements and surcharges according to SGB II, integration services, case management as well as the compilation of statistics and comparison with personal data of the German Federal Employment Agency (BA). OPEN/PROSOZ is used to collect and process personal data of recipients of social assistance or third parties obliged to provide information, to document eligibility requirements, to calculate entitlement to assistance and to issue notices. The scope of services in the case processing includes all the social aids of Book XII of the Social Code, namely help for subsistence (HzL), basic provision for old age and reduced earning capacity (GruSi) as well as the one-off and ongoing aids (aids to health, integration aids for disabled people, aid to care, aid to overcome special social difficulties and help in other life situations). Benefits for the integration of disabled people will be moved from the SGB XII to the scope of application of SGB IX on 01.01.2020. These services will continue to be provided by the municipalities. OPEN/PROSOZ therefore already has the option of setting up these services. In addition, OPEN/PROSOZ also calculates and awards benefits in accordance with SGB II, namely unemployment benefit II and integration benefits in accordance with § 16 et seq. of SGB II. In addition, *OPEN/PROSOZ can be used to calculate and award benefits in accordance with the Asylum Seeker Benefits Act (AsylbLG) and various state laws, such as the state aid for the blind, the state care allowance or the care housing allowance.*

8. Transnational issues:

   OPEN/PROSOZ is currently only used by users in Germany. The system and its data remain completely in the system environment of the respective user within Germany, so that there are currently no transnational processes.

9. Tools used by the manufacturer of the IT product:

   None.

10. Edition of EuroPriSe Criteria used for the evaluation:

    January 2017

11. Evaluation results:

    According to the EuroPriSe Expert, OPEN/PROSOZ meets all data protection and data security requirements.

    Personal data

    It is inherent to the working environment of social benefits that a large amount of personal data must be collected and processed due to legal obligations. OPEN/PROSOZ processes basic data, such as name, contact details, bank details, custody, disability, need for care, earning capacity, household community, etc., as well as case management data (case manager, persons on case, contact management, previous assistance, profile/diagnosis, integration management, phases of unemployment, job search/placement and evaluation) and free text fields. In the process, the processing department (user) is made aware of the obligation to use these free text fields in OPEN/PROSOZ in an earmarked and data-saving manner. Finally, system and protocol data are generated which can contain employee and social data. It cannot be ruled out that the social data processed by OPEN/PROSOZ may also contain health data (such as the sign of severe disability) and thus special categories of personal data pursuant to Art. 9 (1) GDPR.

    Controller

    The OPEN/PROSOZ user decides on the means and purposes of the data processing; this is a social service provider, i.e. an authority or other public body. They are to be classified *as the controller. PROSOZ Herten GmbH, on the other hand, has no access to the system installed on the user's premises, so that there is no processing by a processor.*

PROSOZ Herten GmbH develops and delivers the software to the users (authorities, municipalities). This is done via maintenance and servicing contracts on the basis of EVB-IT maintenance. Within the scope of error correction, it is certainly possible to transmit case data in order to be able to find defects / errors in the specialist application more quickly on the basis of this data. This case data, however, is transferred by default exclusively in anonymous, non-personal form. The functions provided for this purpose ensure that transferred data is completely anonymised. All personal information such as surname, first name, details of place of birth, bank details, etc. are replaced by randomly generated values. A conclusion and/or a restoration of the information with reference to a natural person are not possible.

Legal bases

*The legal basis for the processing of personal data in OPEN/PROSOZ can be found in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, **GDPR**). To the extent that the Member States made use of the opening clauses contained in the GDPR, the basic principles can also be found in national adaptation laws, such as the new **Federal Data Protection Act (BDSG)** for Germany.*

*OPEN/PROSOZ is currently only used by users in Germany. The system and its data remain completely in the system environment of the respective user within Germany, so that there are **no transnational processes** at the time of evaluation.*

According to the opening clause of art. 6 par. 2 and 3 in connection with Art. 6 para. 1 subsec. 1 lit. e GDPR, the sector-specific provisions of the German Social Security Codes (SGB) were also retained in Germany. For this purpose, SGB I and X were editorially revised and adapted to the GDPR. OPEN/PROSOZ serves to process social data in accordance with the sector-specific obligations of social law.

For this, the SGB II, SGB IX, SGB X, SGB XII and other achievement laws are relevant. Relevant are also legal bases for processes of the data synchronization, which are regulated according to § 52 SGB II and §§ 120, 118 SGB XII in ordinances (GrSiDAV or SozhiDAV). OPEN/PROSOZ also processes personal data in accordance with § 67c (1) SGB X within the framework of so-called integration agreements. These are to be evaluated as public law contracts according to § 15 SGB II. On the other hand, the *consent of the person concerned in accordance with Art. 6 para. 1 lit. a GDPR in connection with Recital 43 GDPR is excluded due to the official nature of the processing in OPEN/PROSOZ.*

*When using OPEN/PROSOZ, the controller shall ensure that the need for special protection of children is taken into account when assessing the risks of processing. Social service providers as data controllers must comply with the limits set by law for the processing of **children's data**. These limits are set by sector-specific social legislation. The provisions of German social law do not provide any specific requirements for the processing of data from children or adolescents. Insofar as children's data are processed using OPEN/PROSOZ, the principles of sector-specific social law also apply to these processing operations.*

*In addition, the **data protection laws of the federal states** apply. These regulate areas that are not covered by the GDPR or can be regulated on the basis of opening clauses of the GDPR. One example is the **Hamburg Data Protection Act** (HmbDSG), which regulates, among other things, the protection of employee data in public places.*

*In addition, **interpretation aids** of the European Data Protection Board, the case law of the European Courts and, where applicable, national requirements or interpretation aids of the data protection supervisory authorities must be observed. For OPEN/PROSOZ, for example, the interpretation aid on social data protection of the Bavarian State Commissioner for Data Protection with the title "Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung (DSGVO)" of 25.09.2017 is of importance*[1]*.*

Social data, Social secrecy, Purpose limitation, Necessity

OPEN/PROSOZ is mainly used to process social data. These are according to § 67 Abs. 1 SGB X: „(...) personal data (Article 4(1) of Regulation (EU) 2016/679) processed by a body referred to in Article 35 of the First Book with a view to carrying out its tasks under this Code." When processing social data, the service providers must comply with the social confidentiality of § 35 SGB I. According to this everyone has a right to social data concerning oneself (§ 67 paragraph 2 SGB X) not being processed by the service providers in an unauthorized manner. OPEN/PROSOZ supports this in particular through technical and organisational measures. This is supplemented by the purpose limitation principle of

[1] Cf. the publication of the Bavarian State Commissioner for Data Protection "Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung (DSGVO)" of 25.09.2017, available with status 12/2019 at https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf .

§ 78 SGB X and the necessity principle of § 67c Para. 1 SGB X. With OPEN/PROSOZ, the authorization concept can be made even more differentiated by the individually configurable rights, so that - in accordance with § 35 SGB I - only the responsible processing department within the authority has access to social data to the required extent. In this way, the application meets the special protection requirements of the social data and the separation of purposes.

Anonymizing

In OPEN/PROSOZ it is possible to make the database completely anonymous. To do this, the user creates a copy of the production database. With the function "Anonymize database", all personal data in the database copy is anonymized.

Privacy-by-Design / Default

OPEN/PROSOZ is regularly adapted to the often-changing social laws and the relevant case law of the social courts as well as to the needs of the users. The user is comprehensively informed about the data processing processes in the product documents. In addition, the user is informed and sensitized about data protection and data security. Documents, intuitive user guidance and "read me" in OPEN/PROSOZ promote this. Data protection and security measures comply with the privacy-by-design principle.

Data security

The physical protection of the system components is the sole responsibility of the user, since OPEN/PROSOZ is installed in his IT system environment. Data protection and data security are dealt with comprehensively for the user in a ***concept [SiKo].*** *This concept also provides guidance for action (e.g. password protection). The standard installation provides for a minimum length of 12 characters, a maximum of 3 incorrect logins and a password validity period of 90 days. Since these basic settings can be changed, the [SiKo] contains a note that the current requirements of the German Federal Office for Information Security (BSI) and the (data protection) supervisory authorities must be examined and implemented if possible. After the possible login attempts have been exhausted, the user is automatically blocked; only the administrator in the System Client can remove this block (reassignment of a password, which the user must change immediately after the first login). User passwords are stored encrypted in the database. This ensures adequate protection against unauthorized access to these passwords.*

*The user is responsible for the use of **encryption and signature procedures**. OPEN/PROSOZ supports this by sensitizing the user in [SiKo] to the recommended use of encryption methods. For example, operation in specially protected environments is recommended. In addition to technical and organizational regulations, this also includes the use of encryption and signature procedures provided by the database system used. The MSSQL Server or Oracle database systems can be used for data storage, so that reference is made to the security measures or encryption procedures offered by the manufacturers. OPEN/PROSOZ thus enables the use of encryption and signature procedures between client and database server as well as on the database server itself according to the respective needs of the user and thus offers an appropriate level of protection.*

*The **integrity** of the collected data, i.e. the protection against unauthorized changes, is taken into account both by the allocation of the dedicated access authorizations and by the logging. The user administration implemented in OPEN/PROSOZ clearly regulates the respective areas of responsibility of the users. This clearly defines who may change or delete data: For example, it is not at all possible to delete cases or parts of cases with individual case processing, this is only possible for users with the appropriate authorization in Global Case Processing. The authorization concept is exemplary. In addition, log files log which user was logged on to the application and whether any changes were made to the existing data records.*

*The **confidentiality** of the data is guaranteed by various security measures: On the one hand, the user administration is integrated with corresponding role distribution and login procedure. On the other hand, precautions have also been taken against bypassing the client application: Such bypassing of the clients, i.e. direct access to the database, is not possible without knowing the user name and password for the ODBC connection. However, this access data is stored encrypted in the registry. Finally, the encryption of the communication between database and client can be activated or configured as a function of the database system used, so that the data cannot be compromised during this transfer. This encryption is performed by the database management system and the locally installed driver. It is therefore up to the user to implement this.*

*The **connection of the external appointment management** (Outlook) to OPEN/PROSOZ theoretically enables the disclosure of personal data, which are subject to social secrecy according to § 35 para. 1 SGB I, to third parties. This can happen e.g. by the fact that the Outlook calendar is not only released for the inspection by the editor himself, but is also available to other users in a readable form. In order to adequately* *counter this risk, OPEN/PROSOZ implemented a note that shows the risks during system configuration before the Outlook connection is implemented. In [SiKo], the user is sensitized to the safe handling and possible risks during synchronization. In addition, there is a note on compliance with social secrecy. With the security measures described, an appropriate level of protection can be provided to guarantee the confidentiality of the data.*

Rights of data subjects

The rights of the data subject laid down in the GDPR (and the SGB X) are supported in a variety of ways, e.g. by the security concept, which informs about the user's obligation to comply with the data subject's rights. Furthermore, the operating manuals contain information on the data processing steps so that the user is always in a position to provide information or notify the data subject. Print functions of the data masks in OPEN/PROSOZ additionally support this.

12. Data flow:

OPEN/PROSOZ can be used as a "client / server application" or in a terminal server environment. OPEN/PROSOZ is always integrated into the existing IT landscape of the user, so that the security requirements and operating concepts of the operational environment are adopted. This applies in particular to the encryption established on the database server side for communication between the application and the database, but also to communication between the application and file storage (file server). The following figures illustrate the process.

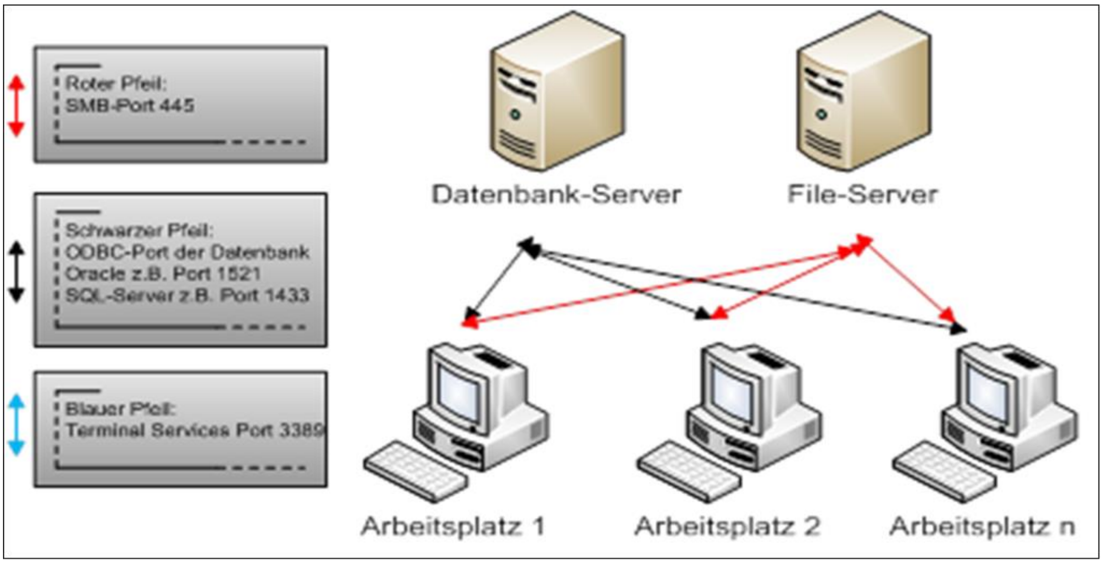

Figure 1: Data flow using the client-server environment

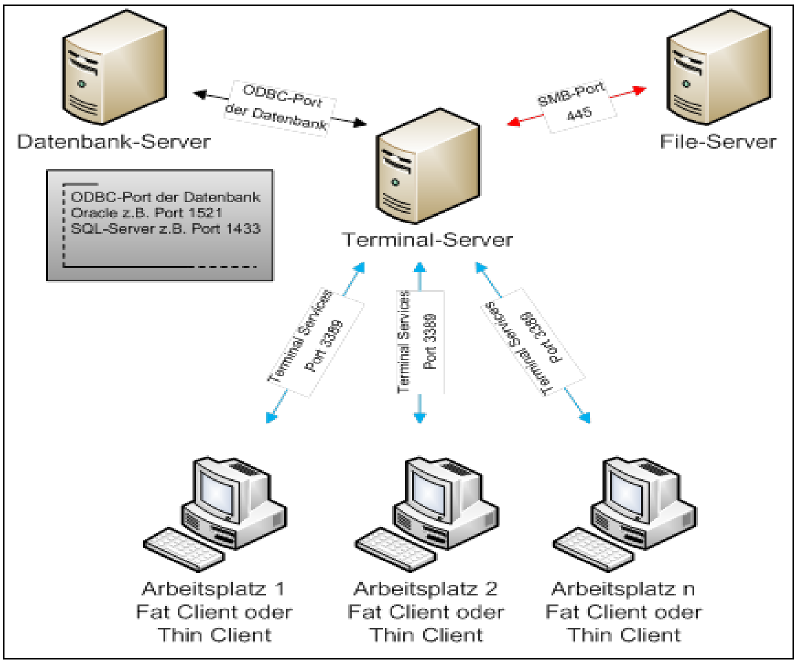

Figure 2: client server structure

13. Privacy-enhancing functionalities:

OPEN/PROSOZ contains the following data protection functions:

• *The database application is characterized by a dedicated authorization and role concept.*

• *Users are sensitized in an exemplary manner by various data protection notices and an intuitive user guidance.*

• *Print functions optimally support access requests from data subjects.*

14. Issues demanding special user attention:

None.

15. Compensation of weaknesses:

Not necessary.

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*adequate*	OPEN/PROSOZ enables the user to process as little personal data as possible and only as much as necessary. However, social data is naturally very extensive. In addition, there are free text fields, which must be used sparingly by the user. The product supports a strictly purpose-related and data-saving handling and provides, for example, an anonymization function as well as an understandable deletion concept.
Transparency	*adequate*	The comprehensive product documentations, in particular the data protection and security concept, disclose all relevant data processing processes and data protection-friendly configurations to the user.
Technical-Organisational Measures	*Adequate, in parts exemplary*	The technical and organisational measures implemented by OPEN/PROSOZ in the system correspond to the state of the art. Many measures must be taken and set up by the user in his own environment when deploying the software. OPEN/PROSOZ supports the user with comprehensive product documentation and a very transparent data protection and security concept with practical instructions.
Data Subjects' Rights	*Adequate, in parts exemplary*	OPEN/PROSOZ enables the user to correctly implement the rights of those affected. In particular, the information functions should be highlighted as exemplary.

Experts' Statement

I affirm that the above-named IT product 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, den *02.12.2019* Irene Karper

Place, date Name of Legal Expert Signature of Legal Expert

Bremen, den *02.12.2019* Irene Karper

Place, date Name of Technical Expert Signature of Technical Expert

Certification Result

The above-named IT product passed the EuroPriSe evaluation.

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

Sebastian Meissner

Digitally signed by Sebastian Meissner
DN: cn=Sebastian Meissner, o=EuroPriSe GmbH, ou=EuroPriSe CA, email=meissner@european-privacy-seal.eu, c=DE
Date: 2019.12.04 12:29:53 +01'00'

Place, Date Name of Certification Authority Signature