Kurzgutachten zur Erteilung eines Datenschutzgütesiegels für das IT-Produkt „OPEN/PROSOZ“

im Auftrag der PROSOZ Herten GmbH

datenschutz cert GmbH
04.08.2016

Inhaltsverzeichnis

1. Vorbemerkung

Mit diesem Kurzgutachten werden die Ergebnisse der Auditierung des IT-Produkts „OPEN/PROSOZ“ in der Version 2015.3.0.0 (kurz „OPEN/PROSOZ“) zusammengefasst.

OPEN/PROSOZ wurde erstmals im Jahre 2007 erfolgreich vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zertifiziert und wurde seit dem regelmäßig re-zertifiziert.

2. Zeitraum der Prüfung

Die Begutachtung erstreckte sich auf den Zeitraum von 01.12.2015 bis 04.08.2016 und beinhaltete neben der konzeptionellen Analyse der zur Verfügung gestellten Unterlagen Mitarbeiterbefragungen, Plausibilitätschecks sowie Besichtigungen des Testsystems von OPEN/PROSOZ.

3. Antragstellerin

Antragstellerin ist die

PROSOZ Herten GmbH
Glashütter Str. 53
01309 Dresden.

als Hersteller des Produkts. Ansprechpartner ist Herr Frank Jüttner.

4. Sachverständiger/Prüfstelle

Sachverständige dieses Gutachtens ist die Prüfstelle

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Irene Karper (Recht). Die Begutachtung wurde durchgeführt von Frau Dr. Irene Karper (Recht) und Herrn Ralf von Rahden (Technik). Die Auditoren wurden unterstützt durch Herrn Oliver Stutz, Leiter der DSGSVO-Prüfstelle der datenschutz nord GmbH.

5. Kurzbezeichnung des IT-Produkts

Begutachtet wird das IT-Produkt „OPEN/PROSOZ“ in der Version 2015.3.0.0, nachfolgend kurz als „OPEN/PROSOZ“ bezeichnet.

6. Beschreibung des IT-Produkts

OPEN/PROSOZ ist ein datenbankbasiertes EDV-Dialogsystem, das von Trägern der Sozialhilfe genutzt wird.

Die Software unterstützt die Sachbearbeitung bei der Abwicklung von Sozialhilfeleistungen. Schwerpunkt ist die Einzelfallbearbeitung von Leistungen nach dem SGB XII. Darüber hinaus ermöglicht OPEN/PROSOZ die Bearbeitung von Bedarfen und –Zuschlägen gemäß SGB II, Leistungen der Eingliederung, das Fallmanagement sowie die Erstellung von Statistiken bzw. den Abgleich mit personenbezogenen Daten der Bundesagentur für Arbeit (BA).

7. Tools, die zur Herstellung des Produkts verwendet wurden

Keine.

8. Zweck und Einsatzbereich

Mit OPEN/PROSOZ werden die Erhebung und Verarbeitung personenbezogener Daten von Empfängern sozialer Hilfen bzw. auskunftspflichtiger Dritter, die Dokumentation der Anspruchsvoraussetzungen, die Berechnung des Hilfeanspruchs und die Bescheiderteilung vorgenommen. Der Leistungsumfang in der Fallbearbeitung umfasst sämtliche sozialen Hilfen des SGB XII, nämlich die Hilfe zum Lebensunterhalt (HzL), die Grundsicherung im Alter und bei Erwerbsminderung (GruSi) sowie die einmaligen und laufenden Hilfen (Hilfen zur Gesundheit, Eingliederungshilfen für behinderte Menschen, Hilfe zur Pflege, Hilfe zur Überwindung besonderer sozialer Schwierigkeiten sowie Hilfe in anderen Lebenslagen). Darüber hinaus werden mit OPEN/PROSOZ Leistungen nach dem SGB II, nämlich Arbeitslosengeld II sowie Eingliederungsleistungen nach § 16ff. SGB II, berechnet und beschieden. Ferner können mit OPEN/PROSOZ Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG) sowie nach verschiedenen Landesgesetzen, wie der Landesblindenhilfe, dem Landespflegegeld oder dem Pflegewohngeld berechnet und beschieden werden.

9. Modellierung des Datenflusses

OPEN/PROSOZ kann als „Client / Server Anwendung“ oder in einer Terminalserverumgebung eingesetzt werden. OPEN/PROSOZ wird dabei immer in die bestehende IT Landschaft des Anwenders integriert, so dass bezüglich der Einsatzumgebung die dortigen Sicherheitsanforderungen und Betriebskonzepte übernommen werden. Dies betrifft insbesondere die datenbankserverseitig etablierte Verschlüsselung für die Kommunikation zwischen der Anwendung und der Datenbank aber auch die Kommunikation zwischen Anwendung und Dateiablage (Fileserver). Die nachfolgenden Abbildungen veranschaulichen den Betrieb.

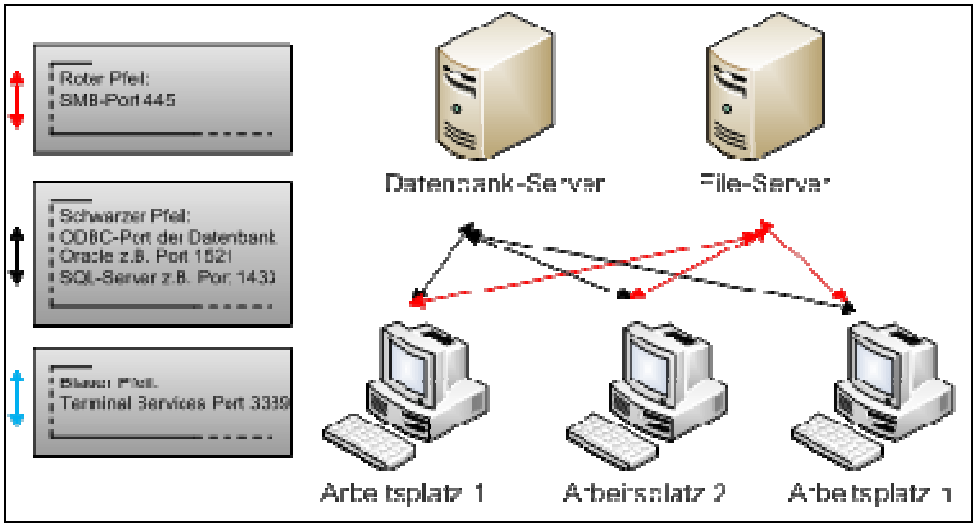


Abbildung 1 Client-Server-Umgebung

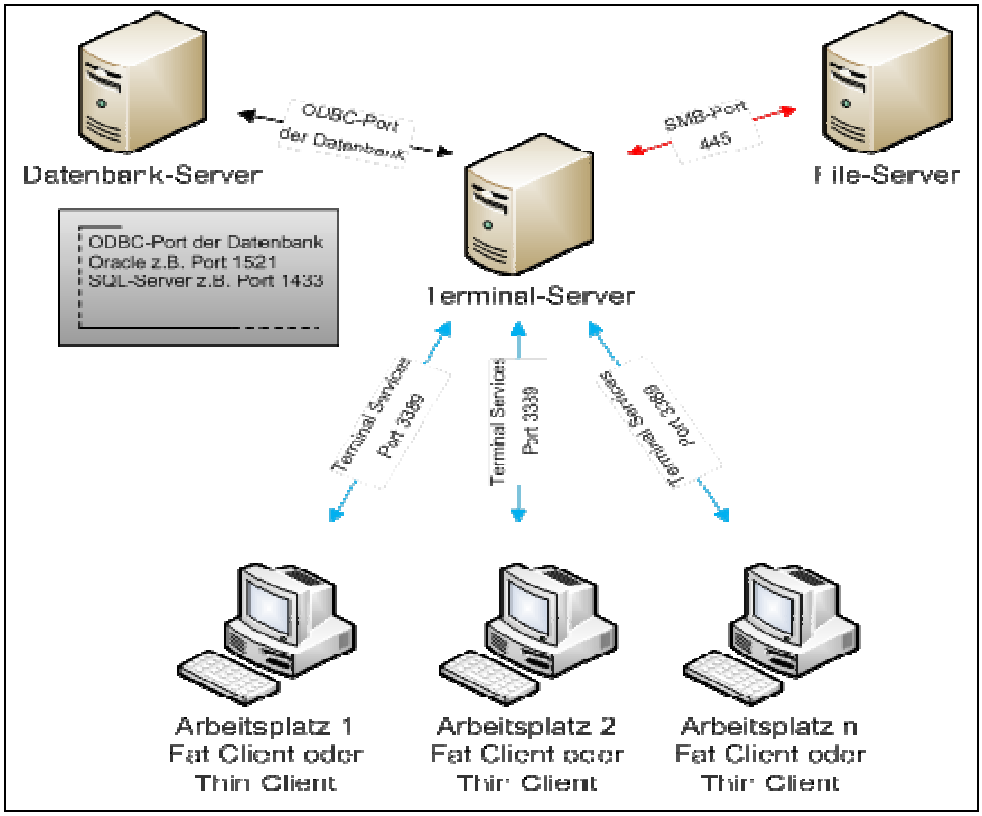


Abbildung 2 Terminalserverumgebung

Der Fatclient kommuniziert über eine verschlüsselte ODBC Verbindung mit dem Datenbanksystem (wahlweise MS-SQL Server oder aber Oracle).

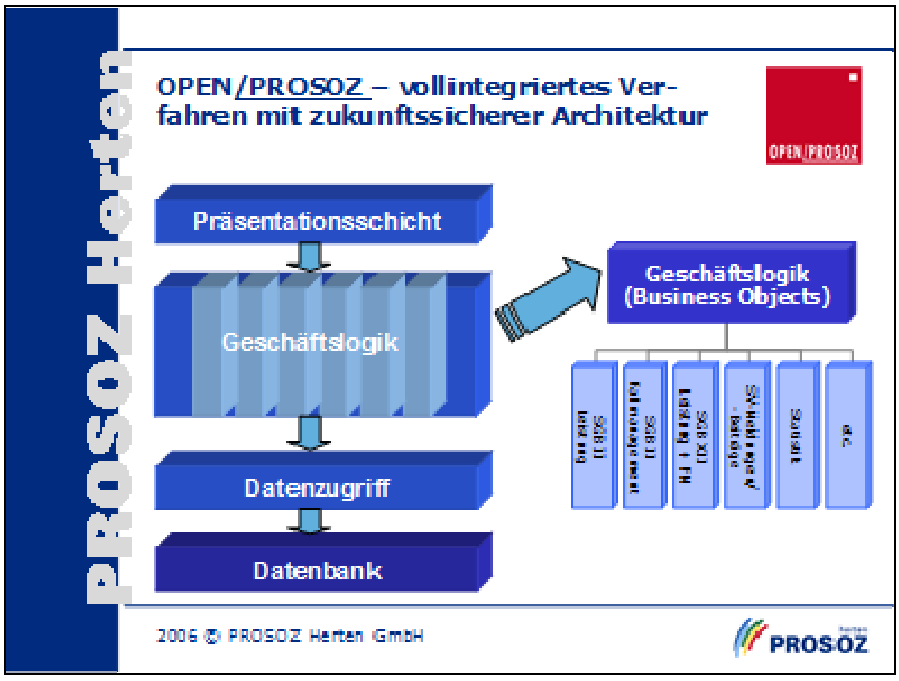


Abbildung 3 Genereller Datenfluss

10. Änderungen seit der letzten Zertifizierung im Überblick

Seit der letzten Zertifizierung des ULD wurde OPEN/PROSOZ vor allem an einige Änderungen des Sozialrechts - und damit verbunden – bezüglich der notwendigen Datenfelder angepasst:

Version 3.14.0

- --- Einführung neuer Assistenten, welche es der Sachbearbeitung ermöglichen, Fallakten über einen Wizard einzustellen bzw. Fallakten wieder aufzunehmen.
- --- Optimierung / Ablösung der bisherigen Funktionalität zum Austausch des zuständigen Mitarbeiters in der Fallakte.
- --- Erweiterung der Termin- und Aufgabenverwaltung. U.a. ist es nun möglich, Termine und Aufgaben den betroffenen Personen und nicht mehr unspezifisch der Fallakte zuzuordnen.
- --- Neue Optionen (Ziel Datensparsamkeit) für Einlesen und Verarbeitung der Rückantworten für den GrSiDAV/SozhiDAV (§ 52 SGB II / § 118 SGB XII).

Version 3.15

- --- Die Anschrift des Zahlungsschuldners wird nun erzwungen, da eine Vielzahl von Kassenverfahren das Vorhandensein einer Anschrift voraussetzt.
- --- Getrennte Leistungsberechnung im Einzelfall / abhängig von der Aufgabenzuordnung kann nun ein Mitarbeiter nur noch die Leistungen berechnen, für welche er direkt zuständig ist.

Version 3.16

- --- Neue Parameter verpflichten durchgängig zur Nutzung von SEPA.
- --- Steuerung von abhängigen Eingabefeldern auf dynamischen Masken.

Version 3.17

- --- Einführung einer Kennworthistorie.

Version 3.18

- --- Einführung des „Statusassistenten“ zur Ermittlung von ALO/ASU Status im Rechtskreis SGB II.

Version 2015.1.0.0

- --- Die Versionierungsbezeichnung wurde verändert (eigentlich 3.19). Die PROSOZ Herten GmbH hat sich entschieden, marktüblich das Jahresdatum voran zu setzen und die Versionen im Jahr durchzunummerieren.
- --- Veränderungen aus den neuen Vorgaben der SGB II Pflichtstatistik („XSOZIAL“).

Version 2015.2.0.0

- --- Bereinigung der Masken und Datenfelder, Anpassung des Bereiches „Kosten der Unterkunft“ an die geltende Rechtsprechung.

Version 2015.3.0.0

--- Änderungen im Bereich der Sozialversicherung / Entfall der Familienversicherung für Berechtigte im SGB II.

Es ist hervorzuheben, dass alle Änderungen, die auch transparent in den jeweiligen Benutzerhandbüchern erklärt werden, keine Auswirkungen auf die bisherige datenschutzrechtliche oder datensicherheits-technische Bewertung haben.

Ferner wird OPEN/PROSOZ nach wie vor ausschließlich in der IT-Umgebung beim Anwender eingesetzt. Maßnahmen der IT-Sicherheit, des organisatorischen Datenschutzes, der Anonymisierung und Pseudonymisierung sowie der Betroffenenrechte sind daher ebenfalls unverändert zu bewerten und entsprechen weiterhin den datenschutzrechtlichen Anforderungen.

11. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 2

12. Zusammenfassung der Prüfergebnisse

Die Prüfergebnisse im Einzelnen werden wie folgt zusammengefasst:

Nr.	Anforderungen nach Katalog oder sonstigen Rechtsnormen	Bewertung
A Allgemeines Anforderungsprofil (Primärdaten):		
	Komplex 1	
A1	1.1 Verfügbarkeit, Integrität, Vertraulichkeit	adäquat
A2	1.2 Nicht-Verkettbarkeit	adäquat
A3	1.3 Transparenz	adäquat
A4	1.4 Intervenierbarkeit	adäquat
A5	1.5 Anpassung des IT-Produkts	adäquat
A6	1.6 Privacy by Default	vorbildlich
A7	1.7 Sonstige Anforderungen	adäquat
	Komplex 2	
A8	2.1 Ermächtigungsgrundlage	adäquat
	2.1.1 Gesetzliche Ermächtigung	adäquat
	2.1.2 Einwilligung des Betroffenen	adäquat
	2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung	adäquat
	2.1.3.1 Vorschriften über die Datenerhebung	adäquat
	2.1.3.2 Vorschriften über die Übermittlung	adäquat
	2.1.3.3 Löschung nach Wegfall des Erfordernisses	adäquat

A9	2.2 Einhaltung allg. Datenschutzgrundsätze und Pflichten	adäquat
	2.2.1 Zweckbindung und Zweckänderung	vorbildlich
	2.2.2 Erleichterung der Umsetzung des Trennungsgebots	adäquat
	2.2.3 Gewährleistung der Datensicherheit	adäquat
A10	2.3 Datenverarbeitung im Auftrag	n.a.
A11	2.4 Voraussetzungen besonderer technischer Verfahren	n.a.
	2.4.1 Gemeinsames Verfahren / Abrufverfahren	n.a.
	2.4.2 Trennung der Verantwortlichkeiten	n.a.
	2.4.3 Veröffentlichungen im Internet	n.a.
	2.4.4 Weitere besondere technische Verfahren	n.a.
	2.4.1 Gemeinsames Verfahren / Abrufverfahren	n.a.
A12	2.5 Sonstige Anforderungen	n.a.
	2.5.1 Unterstützung Pseudonymität / Pseudonymisieren	n.a.
	Komplex 3	
A13	3.1 Einzelne technisch-organisatorische Maßnahmen	adäquat
	3.1.1 Physikalische Sicherung	adäquat
	3.1.2 Authentisierung	adäquat
	3.1.3 Autorisierung	vorbildlich
	3.1.4 Protokollierung	adäquat
	3.1.5 Verschlüsselung und Signatur	adäquat
	3.1.6 Pseudonymisierung	adäquat
	3.1.7 Anonymisierung	adäquat
A14	3.2 Allgemeine Pflichten	adäquat
	3.2.1 Technisch-Organisatorische Maßnahmen	adäquat
	3.2.1.1 Verfügbarkeit	adäquat
	3.2.1.2 Integrität	vorbildlich
	3.2.1.3 Vertraulichkeit	adäquat
	3.2.1.4 Nicht-Verkettbarkeit	adäquat
	3.2.1.5 Transparenz	adäquat
	3.2.1.6 Intervenierbarkeit	adäquat
	3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	adäquat
	3.2.1.8 Test und Freigabe	adäquat

	3.2.2 Erleichterung der Vorabkontrolle	adäquat
	3.2.3 Erleichterung der Erstellung von Verfahrensverzeichnissen	adäquat
	3.2.4 Benachrichtigungspflicht	adäquat
	3.2.5 Unterstützung behördlicher Datenschutzbeauftragter	adäquat
A15	3.3 Spezifische Pflichten	adäquat
	3.3.1 Verschlüsselung	adäquat
	3.3.2 Anonymisierung oder Pseudonymisierung	adäquat
	3.3.3 Spezielle Anforderungen bei besonderem Technikeinsatz	n.a.
	3.3.3.1 Mobile Datenverarbeitungssysteme	n.a.
	3.3.3.2 Video-Überwachung und –Aufzeichnung	n.a.
	3.3.3.3 Automatisierte Einzelentscheidungen	n.a.
	3.3.3.4 Veröffentlichungen im Internet	n.a.
A16	3.4 Pflichten nach DSVO	adäquat
A17	3.5 Anforderungen beim Betrieb der Auftragsdatenverarbeitung	n.a.
A18	3.6 Sonstige Anforderungen	n.a.
	Komplex 4	
A19	4.1Aufklärung und Benachrichtigung	adäquat
A20	4.2Benachrichtigung bei unrechtmäßiger Kenntniserlangung	adäquat
A21	4.3Auskunft	adäquat
A22	4.4 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	adäquat
	4.4.1 Berichtigung	adäquat
	4.4.2 Vollständige Löschung	adäquat
	4.4.3 Sperrung	adäquat
	4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	n.a.
	4.4.5 Gegendarstellung	n.a.
A23	4.5 Sonstige Anforderungen	n.a.

Nr.	**Anforderungen nach Katalog oder sonstigen Rechtsnormen**	**Bewertung**
	B Anforderungsprofil für Protokolldaten (Sekundärdaten):	
	Komplex 1	
B1	1.1 Datenvermeidung und Datensparsamkeit	adäquat

B2	1.2 Zweckbindung	vorbildlich
B3	1.3 Nicht-Verkettbarkeit	adäquat
B4	1.4 Transparenz	adäquat
	1.5 Sonstige Anforderungen	n.a.
	Komplex 2	
B5	2.1 Rechtsgrundlagen	adäquat
B6	2.2 Zweckbindung	vorbildlich
B7	2.3 Aufbewahrungsfristen und Löschung	adäquat
	2.4 Sonstige Anforderungen	n.a.
	Komplex 3	
B8	3.1 Physikalische Sicherung	adäquat
B9	3.2 Zugriffsschutz	adäquat
B10	3.3 Ermittlung / Informationsgehalt	adäquat
	3.4 Sichtbarkeit der Protokolldaten	adäquat
B11	3.5 Technische Umsetzung der Speicherfristen	adäquat
B12	3.6 Unzulässige Verkettung	adäquat
B13	3.7 Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	adäquat
	Sonstige Anforderungen	n.a.
	Komplex 4	
B14	4.1 Selektive Löschung von Einzeldaten	adäquat
	4.2 Beauskunftung	adäquat
	4.3 Berichtigung	adäquat
	4.4 Sperrung	adäquat
	4.5 Einwand	n.a.

13. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das IT-Produkt OPEN/PROSOZ fördert den Datenschutz auf vielfältige Weise:

--- Die Datenbankanwendung zeichnet sich durch ein dediziertes Berechtigungs- und Rollenkonzept aus.

--- Benutzer werden durch verschiedene Datenschutzhinweise und eine intuitive Benutzerführung vorbildlich sensibilisiert.

--- Druckfunktionen unterstützen Auskunftsbegehren von Betroffenen optimal.

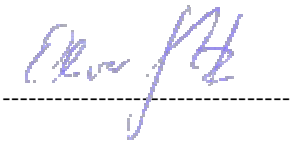
14. Votum der Auditoren

OPEN/PROSOZ setzt insgesamt die Anforderungen an den Datenschutz angemessen um.

Bremen, den 04.08.2016.

Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH



Oliver Stutz
datenschutz nord GmbH